XGS-4528F

Intelligent Layer 3+ Switch

User's Guide

Version 3.80
8/2007
Edition 1

DEFAULT LOGIN	
IP Address	**http://192.168.1.1**
User Name	**admin**
Password	**1234**

ZyXEL

www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the Switch using the web configurator or via commands. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide
  The Quick Start Guide contains information on setting up your hardware.
- Web Configurator Online Help
  Embedded web help for descriptions of individual screens and supplementary information.

It is recommended you use the web configurator to configure the Switch.

- Supporting Disk
  Refer to the included CD for support documents.
- ZyXEL Web Site
  Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

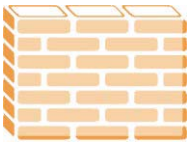
Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The XGS-4528F may be referred to as the "Switch", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The Switch icon is not an exact representation of your device.

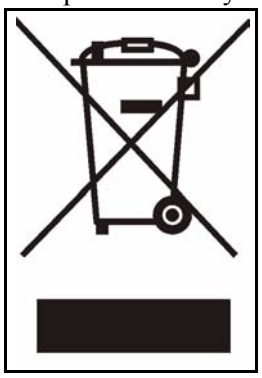
The Switch	Computer	Notebook computer
Server	DSLAM	Firewall 
Telephone	Switch	Router

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- For continued protection against risk of fire replace only with same type and rating of fuse.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.

This product is recyclable. Dispose of it properly.



Contents Overview

Introduction 33

Getting to Know Your Switch 35
Hardware Installation and Connection 39
Hardware Overview 43

Basic Configuration 49

The Web Configurator 51
Initial Setup Example 61
System Status and Port Statistics 67
Basic Setting 73

Advanced Setup 85

VLAN 87
Static MAC Forward Setup 103
Filtering 105
Spanning Tree Protocol 107
Bandwidth Control 127
Broadcast Storm Control 129
Mirroring 131
Link Aggregation 133
Port Authentication 141
Port Security 147
Classifier 151
Policy Rule 157
Queuing Method 163
VLAN Stacking 167
Multicast 173
Authentication & Accounting 187
IP Source Guard 201
Loop Guard 221

IP Application 225

Static Route 227
RIP 229
OSPF 231
IGMP 243
DVMRP 247

Differentiated Services 251
DHCP 259
VRRP 267

Management 277

Maintenance 279
Access Control 285
Diagnostic 303
Syslog 305
Cluster Management 309
MAC Table 315
IP Table 317
ARP Table 319
Routing Table 321
Configure Clone 323

Troubleshooting & Product Specifications 325

Troubleshooting 327
Product Specifications 335

Appendices and Index 343

Table of Contents

About This User's Guide **3**

Document Conventions **4**

Safety Warnings **6**

Contents Overview **9**

Table of Contents **11**

List of Figures **23**

List of Tables **29**

Part I: Introduction **33**

Chapter 1
Getting to Know Your Switch **35**

1.1 Introduction 35
1.1.1 Bridging Example 35
1.1.2 High Performance Switching Example 36
1.1.3 Gigabit Ethernet to the Desktop 37
1.1.4 IEEE 802.1Q VLAN Application Example 37
1.2 Ways to Manage the Switch 38
1.3 Good Habits for Managing the Switch 38

Chapter 2
Hardware Installation and Connection **39**

2.1 Freestanding Installation 39
2.2 Mounting the Switch on a Rack 40
2.2.1 Rack-mounted Installation Requirements 40
2.2.2 Attaching the Mounting Brackets to the Switch 40
2.2.3 Mounting the Switch on a Rack 41

Chapter 3
Hardware Overview **43**

3.1 Front Panel Connections 43
3.1.1 Dual Personality Interfaces 43
3.1.2 1000Base-T Ports 44

3.1.3 Mini-GBIC Slots 44
3.2 Rear Panel 46
3.2.1 Power Connector 47
3.2.2 External Backup Power Supply Connector 47
3.2.3 Console Port 47
3.3 LEDs 47

Part II: Basic Configuration 49

Chapter 4
The Web Configurator 51

4.1 Introduction 51
4.2 System Login 51
4.3 The Status Screen 52
4.3.1 Change Your Password 58
4.4 Saving Your Configuration 58
4.5 Switch Lockout 58
4.6 Resetting the Switch 59
4.6.1 Reload the Configuration File 59
4.7 Logging Out of the Web Configurator 60
4.8 Help 60

Chapter 5
Initial Setup Example 61

5.1 Overview 61
5.1.1 Configuring an IP Interface 61
5.1.2 Configuring DHCP Server Settings 62
5.1.3 Creating a VLAN 63
5.1.4 Setting Port VID 64
5.1.5 Enabling RIP 65

Chapter 6
System Status and Port Statistics 67

6.1 Overview 67
6.2 Port Status Summary 67
6.2.1 Status: Port Details 68

Chapter 7
Basic Setting 73

7.1 Overview 73
7.2 System Information 73

7.3 General Setup 75
7.4 Introduction to VLANs 77
7.5 Switch Setup Screen 77
7.6 IP Setup 79
7.6.1 IP Interfaces 79
7.7 Port Setup 81

Part III: Advanced Setup 85

Chapter 8
VLAN 87

8.1 Introduction to IEEE 802.1Q Tagged VLANs 87
8.1.1 Forwarding Tagged and Untagged Frames 87
8.2 Automatic VLAN Registration 88
8.2.1 GARP 88
8.2.2 GVRP 88
8.3 Port VLAN Trunking 89
8.4 Select the VLAN Type 89
8.5 Static VLAN 89
8.5.1 Static VLAN Status 90
8.5.2 Static VLAN Details 90
8.5.3 Configure a Static VLAN 91
8.5.4 Configure VLAN Port Settings 92
8.6 Subnet Based VLANs 94
8.7 Configuring Subnet Based VLAN 95
8.8 Protocol Based VLANs 96
8.9 Configuring Protocol Based VLAN 97
8.10 Create an IP-based VLAN Example 98
8.11 Port-based VLAN Setup 99
8.11.1 Configure a Port-based VLAN 100

Chapter 9
Static MAC Forward Setup 103

9.1 Overview 103
9.2 Configuring Static MAC Forwarding 103

Chapter 10
Filtering 105

10.1 Configure a Filtering Rule 105

Chapter 11
Spanning Tree Protocol 107

11.1 STP/RSTP Overview 107
11.1.1 STP Terminology 107
11.1.2 How STP Works 108
11.1.3 STP Port States 108
11.1.4 Multiple RSTP 109
11.1.5 Multiple STP 109
11.2 Spanning Tree Protocol Status Screen 112
11.3 Spanning Tree Configuration 113
11.4 Configure Rapid Spanning Tree Protocol 114
11.5 Rapid Spanning Tree Protocol Status 116
11.6 Configure Multiple Rapid Spanning Tree Protocol 117
11.7 Multiple Rapid Spanning Tree Protocol Status 119
11.8 Configure Multiple Spanning Tree Protocol 120
11.9 Multiple Spanning Tree Protocol Status 123

Chapter 12
Bandwidth Control 127

12.1 Bandwidth Control Overview 127
12.1.1 CIR and PIR 127
12.2 Bandwidth Control Setup 127

Chapter 13
Broadcast Storm Control 129

13.1 Broadcast Storm Control Setup 129

Chapter 14
Mirroring 131

14.1 Port Mirroring Setup 131

Chapter 15
Link Aggregation 133

15.1 Link Aggregation Overview 133
15.2 Dynamic Link Aggregation 133
15.2.1 Link Aggregation ID 134
15.3 Link Aggregation Status 134
15.4 Link Aggregation Setting 135
15.5 Link Aggregation Control Protocol 136
15.6 Static Trunking Example 138

Chapter 16
Port Authentication 141

16.1 Port Authentication Overview 141
16.1.1 IEEE 802.1x Authentication 141

16.1.2 MAC Authentication 142
16.2 Port Authentication Configuration 143
16.2.1 Activate IEEE 802.1x Security 143
16.2.2 Activate MAC Authentication 144

Chapter 17
Port Security 147

17.1 About Port Security 147
17.2 Port Security Setup 147

Chapter 18
Classifier 151

18.1 About the Classifier and QoS 151
18.2 Configuring the Classifier 151
18.3 Viewing and Editing Classifier Configuration 154
18.4 Classifier Example 155

Chapter 19
Policy Rule 157

19.1 Policy Rules Overview 157
19.1.1 DiffServ 157
19.1.2 DSCP and Per-Hop Behavior 157
19.2 Configuring Policy Rules 158
19.3 Viewing and Editing Policy Configuration 160
19.4 Policy Example 160

Chapter 20
Queuing Method 163

20.1 Queuing Method Overview 163
20.1.1 Strictly Priority 163
20.1.2 Weighted Fair Queuing 163
20.1.3 Weighted Round Robin Scheduling (WRR) 164
20.2 Configuring Queuing 164

Chapter 21
VLAN Stacking 167

21.1 VLAN Stacking Overview 167
21.1.1 VLAN Stacking Example 167
21.2 VLAN Stacking Port Roles 168
21.3 VLAN Tag Format 169
21.3.1 Frame Format 169
21.4 Configuring VLAN Stacking 170

Chapter 22
Multicast 173

22.1 Multicast Overview 173
22.1.1 IP Multicast Addresses 173
22.1.2 IGMP Filtering 173
22.1.3 IGMP Snooping 173
22.1.4 IGMP Snooping and VLANs 174
22.2 Multicast Status 174
22.3 Multicast Setting 174
22.4 IGMP Snooping VLAN 177
22.5 IGMP Filtering Profile 178
22.6 MVR Overview 179
22.6.1 Types of MVR Ports 180
22.6.2 MVR Modes 180
22.6.3 How MVR Works 180
22.7 General MVR Configuration 181
22.8 MVR Group Configuration 183
22.8.1 MVR Configuration Example 184

Chapter 23
Authentication & Accounting 187

23.1 Authentication, Authorization and Accounting 187
23.1.1 Local User Accounts 187
23.1.2 RADIUS and TACACS+ 188
23.2 Authentication and Accounting Screens 188
23.2.1 RADIUS Server Setup 188
23.2.2 TACACS+ Server Setup 190
23.2.3 Authentication and Accounting Setup 192
23.2.4 Vendor Specific Attribute 195
23.2.5 Tunnel Protocol Attribute 196
23.3 Supported RADIUS Attributes 196
23.3.1 Attributes Used for Authentication 197
23.3.2 Attributes Used for Accounting 197

Chapter 24
IP Source Guard 201

24.1 IP Source Guard Overview 201
24.1.1 DHCP Snooping Overview 201
24.1.2 ARP Inspection Overview 203
24.2 IP Source Guard 205
24.3 IP Source Guard Static Binding 205
24.4 DHCP Snooping 207
24.5 DHCP Snooping Configure 210

24.5.1 DHCP Snooping Port Configure 211
24.5.2 DHCP Snooping VLAN Configure 213
24.6 ARP Inspection Status 214
24.6.1 ARP Inspection VLAN Status 214
24.6.2 ARP Inspection Log Status 215
24.7 ARP Inspection Configure 217
24.7.1 ARP Inspection Port Configure 218
24.7.2 ARP Inspection VLAN Configure 219

Chapter 25
Loop Guard 221

25.1 Loop Guard Overview 221
25.2 Loop Guard Setup 223

Part IV: IP Application 225

Chapter 26
Static Route 227

26.1 Configuring Static Routing 227

Chapter 27
RIP 229

27.1 RIP Overview 229
27.2 Configuring RIP 229

Chapter 28
OSPF 231

28.1 OSPF Overview 231
28.1.1 OSPF Autonomous Systems and Areas 231
28.1.2 How OSPF Works 232
28.1.3 Interfaces and Virtual Links 232
28.1.4 OSPF and Router Elections 232
28.1.5 Configuring OSPF 233
28.2 OSPF Status 233
28.3 OSPF Configuration 235
28.4 Configure OSPF Areas 237
28.4.1 View OSPF Area Information Table 238
28.5 Configuring OSPF Interfaces 238
28.6 OSPF Virtual-Links 240

Chapter 29
IGMP 243

29.1 IGMP Overview 243
29.1.1 How IGMP Works 244
29.2 Port-based IGMP 245
29.3 Configuring IGMP 245

Chapter 30
DVMRP 247

30.1 DVMRP Overview 247
30.2 How DVMRP Works 247
30.2.1 DVMRP Terminology 248
30.3 Configuring DVMRP 248
30.3.1 DVMRP Configuration Error Messages 249
30.4 Default DVMRP Timer Values 250

Chapter 31
Differentiated Services 251

31.1 DiffServ Overview 251
31.1.1 DSCP and Per-Hop Behavior 251
31.1.2 DiffServ Network Example 252
31.2 Two Rate Three Color Marker Traffic Policing 252
31.2.1 TRTCM - Color-blind Mode 253
31.2.2 TRTCM - Color-aware Mode 253
31.3 Activating DiffServ 254
31.3.1 Configuring 2-Rate 3 Color Marker Settings 254
31.4 DSCP-to-IEEE 802.1p Priority Settings 256
31.4.1 Configuring DSCP Settings 256

Chapter 32
DHCP 259

32.1 DHCP Overview 259
32.1.1 DHCP Modes 259
32.1.2 DHCP Configuration Options 259
32.2 DHCP Status 260
32.3 DHCP Server Status Detail 260
32.4 DHCP Relay 261
32.4.1 DHCP Relay Agent Information 261
32.4.2 Configuring DHCP Global Relay 262
32.4.3 Global DHCP Relay Configuration Example 263
32.5 Configuring DHCP VLAN Settings 264
32.5.1 Example: DHCP Relay for Two VLANs 266

Chapter 33
VRRP 267

33.1 VRRP Overview 267
33.2 VRRP Status 268
33.3 VRRP Configuration 268
33.3.1 IP Interface Setup 268
33.3.2 VRRP Parameters 270
33.3.3 Configuring VRRP Parameters 270
33.3.4 Configuring VRRP Parameters 271
33.4 VRRP Configuration Examples 272
33.4.1 One Subnet Network Example 272
33.4.2 Two Subnets Example 273

Part V: Management 277

Chapter 34
Maintenance 279

34.1 The Maintenance Screen 279
34.2 Load Factory Default 280
34.3 Save Configuration 280
34.4 Reboot System 281
34.5 Firmware Upgrade 281
34.6 Restore a Configuration File 282
34.7 Backup a Configuration File 282
34.8 FTP Command Line 283
34.8.1 Filename Conventions 283
34.8.2 FTP Command Line Procedure 283
34.8.3 GUI-based FTP Clients 284
34.8.4 FTP Restrictions 284

Chapter 35
Access Control 285

35.1 Access Control Overview 285
35.2 The Access Control Main Screen 285
35.3 About SNMP 286
35.3.1 SNMP v3 and Security 287
35.3.2 Supported MIBs 287
35.3.3 SNMP Traps 287
35.3.4 Configuring SNMP 290
35.3.5 Configuring SNMP Trap Group 292
35.3.6 Setting Up Login Accounts 293
35.4 SSH Overview 295
35.5 How SSH works 295

35.6 SSH Implementation on the Switch 296
35.6.1 Requirements for Using SSH 296
35.7 Introduction to HTTPS 296
35.8 HTTPS Example 297
35.8.1 Internet Explorer Warning Messages 297
35.8.2 Netscape Navigator Warning Messages 298
35.8.3 The Main Screen 298
35.9 Service Port Access Control 299
35.10 Remote Management 300

Chapter 36
Diagnostic 303

36.1 Diagnostic 303

Chapter 37
Syslog 305

37.1 Syslog Overview 305
37.2 Syslog Setup 305
37.3 Syslog Server Setup 306

Chapter 38
Cluster Management 309

38.1 Clustering Management Status Overview 309
38.2 Cluster Management Status 310
38.2.1 Cluster Member Switch Management 311
38.3 Clustering Management Configuration 312

Chapter 39
MAC Table 315

39.1 MAC Table Overview 315
39.2 Viewing the MAC Table 316

Chapter 40
IP Table 317

40.1 IP Table Overview 317
40.2 Viewing the IP Table 318

Chapter 41
ARP Table 319

41.1 ARP Table Overview 319
41.1.1 How ARP Works 319
41.2 Viewing the ARP Table 319

Chapter 42
Routing Table 321

42.1 Overview 321
42.2 Viewing the Routing Table Status 321

Chapter 43
Configure Clone 323

43.1 Configure Clone 323

Part VI: Troubleshooting & Product Specifications 325

Chapter 44
Troubleshooting 327

44.1 Problems Starting Up the Switch 327
44.2 Problems Accessing the Switch 327
44.2.1 Pop-up Windows, JavaScripts and Java Permissions 328
44.3 Problems with the Password 333

Chapter 45
Product Specifications 335

Part VII: Appendices and Index 343

Appendix A IP Addresses and Subnetting 345

Appendix B Legal Information 353

Appendix C Customer Support 357

Index 363

List of Figures

Figure 1 Bridging Application 36
Figure 2 High Performance Switching 36
Figure 3 Gigabit to the Desktop 37
Figure 4 Shared Server Using VLAN Example 38
Figure 5 Attaching Rubber Feet 39
Figure 6 Attaching the Mounting Brackets 40
Figure 7 Mounting the Switch on a Rack 41
Figure 8 Front Panel 43
Figure 9 Transceiver Installation Example 45
Figure 10 Installed Transceiver 45
Figure 11 Opening the Transceiver's Latch Example 45
Figure 12 Transceiver Removal Example 45
Figure 13 Rear Panel - AC Model 46
Figure 14 Rear Panel - DC Model 46
Figure 15 Web Configurator: Login 52
Figure 16 Web Configurator Home Screen (Status) 52
Figure 17 Change Administrator Login Password 58
Figure 18 Resetting the Switch: Via the Console Port 60
Figure 19 Web Configurator: Logout Screen 60
Figure 20 Initial Setup Network Example: IP Interface 61
Figure 21 Initial Setup Network Example: VLAN 63
Figure 22 Initial Setup Network Example: Port VID 64
Figure 23 Status 67
Figure 24 Status: Port Details 69
Figure 25 Basic Setting > System Info 74
Figure 26 Basic Setting > General Setup 75
Figure 27 Basic Setting > Switch Setup 78
Figure 28 Basic Setting > IP Setup 80
Figure 29 Basic Setting > Port Setup 82
Figure 30 Port VLAN Trunking 89
Figure 31 Switch Setup: Select VLAN Type 89
Figure 32 Advanced Application > VLAN: VLAN Status 90
Figure 33 Advanced Application > VLAN > VLAN Detail 90
Figure 34 Advanced Application > VLAN > Static VLAN 91
Figure 35 Advanced Application > VLAN > VLAN Port Setting 93
Figure 36 Subnet Based VLAN Application Example 94
Figure 37 Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN 95
Figure 38 Protocol Based VLAN Application Example 97

Figure 39 Advanced Application > VLAN > VLAN Port Setting > Protocol Based VLAN 97
Figure 40 Protocol Based VLAN Configuration Example 99
Figure 41 Advanced Application > VLAN > Port Based VLAN Setup (All Connected) 100
Figure 42 Advanced Application > VLAN: Port Based VLAN Setup (Port Isolation) 101
Figure 43 Advanced Application > Static MAC Forwarding 103
Figure 44 Advanced Application > Filtering 105
Figure 45 MRSTP Network Example 109
Figure 46 STP/RSTP Network Example 110
Figure 47 MSTP Network Example 111
Figure 48 MSTIs in Different Regions 112
Figure 49 MSTP and Legacy RSTP Network Example 112
Figure 50 Advanced Application > Spanning Tree Protocol 113
Figure 51 Advanced Application > Spanning Tree Protocol > Configuration 113
Figure 52 Advanced Application > Spanning Tree Protocol > RSTP 114
Figure 53 Advanced Application > Spanning Tree Protocol > Status: RSTP 116
Figure 54 Advanced Application > Spanning Tree Protocol > MRSTP 117
Figure 55 Advanced Application > Spanning Tree Protocol > Status: MRSTP 119
Figure 56 Advanced Application > Spanning Tree Protocol > MSTP 121
Figure 57 Advanced Application > Spanning Tree Protocol > Status: MSTP 124
Figure 58 Advanced Application > Bandwidth Control 128
Figure 59 Advanced Application > Broadcast Storm Control 129
Figure 60 Advanced Application > Mirroring 131
Figure 61 Advanced Application > Link Aggregation Status 134
Figure 62 Advanced Application > Link Aggregation > Link Aggregation Setting 135
Figure 63 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP 137
Figure 64 Trunking Example - Physical Connections 138
Figure 65 Trunking Example - Configuration Screen 139
Figure 66 IEEE 802.1x Authentication Process 142
Figure 67 MAC Authentication Process 142
Figure 68 Advanced Application > Port Authentication 143
Figure 69 Advanced Application > Port Authentication > 802.1x 143
Figure 70 Advanced Application > Port Authentication > MAC Authentication 145
Figure 71 Advanced Application > Port Security 148
Figure 72 Advanced Application > Classifier 152
Figure 73 Advanced Application > Classifier: Summary Table 154
Figure 74 Classifier: Example 155
Figure 75 Advanced Application > Policy Rule 158
Figure 76 Advanced Application > Policy Rule: Summary Table 160
Figure 77 Policy Example 161
Figure 78 Advanced Application > Queuing Method 164
Figure 79 VLAN Stacking Example 168
Figure 80 Advanced Application > VLAN Stacking 170
Figure 81 Advanced Application > Multicast 174

Figure 82 Advanced Application > Multicast > Multicast Setting 175
Figure 83 Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN 177
Figure 84 Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile 178
Figure 85 MVR Network Example 180
Figure 86 MVR Multicast Television Example 181
Figure 87 Advanced Application > Multicast > Multicast Setting > MVR 182
Figure 88 Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration 184
Figure 89 MVR Configuration Example 185
Figure 90 MVR Configuration Example 185
Figure 91 MVR Group Configuration Example 186
Figure 92 MVR Group Configuration Example 186
Figure 93 AAA Server 187
Figure 94 Advanced Application > Auth and Acct 188
Figure 95 Advanced Application > Auth and Acct > RADIUS Server Setup 189
Figure 96 Advanced Application > Auth and Acct > TACACS+ Server Setup 191
Figure 97 Advanced Application > Auth and Acct > Auth and Acct Setup 193
Figure 98 DHCP Snooping Database File Format 202
Figure 99 Example: Man-in-the-middle Attack 203
Figure 100 IP Source Guard 205
Figure 101 IP Source Guard Static Binding 206
Figure 102 DHCP Snooping 207
Figure 103 DHCP Snooping Configure 210
Figure 104 DHCP Snooping Port Configure 212
Figure 105 DHCP Snooping VLAN Configure 213
Figure 106 ARP Inspection Status 214
Figure 107 ARP Inspection VLAN Status 215
Figure 108 ARP Inspection Log Status 216
Figure 109 ARP Inspection Configure 217
Figure 110 ARP Inspection Port Configure 218
Figure 111 ARP Inspection VLAN Configure 219
Figure 112 Loop Guard vs STP 221
Figure 113 Switch in Loop State 222
Figure 114 Loop Guard - Probe Packet 222
Figure 115 Loop Guard - Network Loop 222
Figure 116 Advanced Application > Loop Guard 223
Figure 117 IP Application > Static Routing 227
Figure 118 IP Application > RIP 230
Figure 119 OSPF Network Example 232
Figure 120 OSPF Router Election Example 233
Figure 121 IP Application > OSPF Status 234
Figure 122 IP Application > OSPF Configuration: Activating and General Settings 236
Figure 123 IP Application > OSPF Configuration: Area Setup 237
Figure 124 IP Application > OSPF Configuration: Summary Table 238

Figure 125 IP Application > OSPF Configuration > OSPF Interface 239
Figure 126 IP Application > OSPF Configuration > OSPF Virtual Link 240
Figure 127 IP Multicast 243
Figure 128 IGMP Version 1 Example 244
Figure 129 IGMP Version 2 Example 245
Figure 130 IGMP Version 3 Example 245
Figure 131 IP Application > IGMP 246
Figure 132 How DVMRP Works 248
Figure 133 IP Application > DVMRP 248
Figure 134 DVMRP: IGMP/RIP Not Set Error 249
Figure 135 DVMRP: Unable to Disable IGMP Error 249
Figure 136 DVMRP: Duplicate VID Error Message 250
Figure 137 DiffServ: Differentiated Service Field 251
Figure 138 DiffServ Network 252
Figure 139 TRTCM - Color-blind Mode 253
Figure 140 TRTCM - Color-aware Mode 253
Figure 141 IP Application > DiffServ 254
Figure 142 IP Application > DiffServ > 2-rate 3 Color Marker 255
Figure 143 IP Application > DiffServ > DSCP Setting 256
Figure 144 IP Application > DHCP Status 260
Figure 145 IP Application > DHCP > DHCP Server Status Detail 260
Figure 146 IP Application > DHCP > Global 262
Figure 147 Global DHCP Relay Network Example 263
Figure 148 DHCP Relay Configuration Example 263
Figure 149 IP Application > DHCP > VLAN 264
Figure 150 DHCP Relay for Two VLANs 266
Figure 151 DHCP Relay for Two VLANs Configuration Example 266
Figure 152 VRRP: Example 1 267
Figure 153 IP Application > VRRP Status 268
Figure 154 IP Application > VRRP Configuration > IP Interface 269
Figure 155 IP Application > VRRP Configuration > VRRP Parameters 271
Figure 156 VRRP Configuration: Summary 272
Figure 157 VRRP Configuration Example: One Virtual Router Network 272
Figure 158 VRRP Example 1: VRRP Parameter Settings on Switch A 273
Figure 159 VRRP Example 1: VRRP Parameter Settings on Switch B 273
Figure 160 VRRP Example 1: VRRP Status on Switch A 273
Figure 161 VRRP Example 1: VRRP Status on Switch B 273
Figure 162 VRRP Configuration Example: Two Virtual Router Network 274
Figure 163 VRRP Example 2: VRRP Parameter Settings for VR2 on Switch A 274
Figure 164 VRRP Example 2: VRRP Parameter Settings for VR2 on Switch B 274
Figure 165 VRRP Example 2: VRRP Status on Switch A 275
Figure 166 VRRP Example 2: VRRP Status on Switch B 275
Figure 167 Management > Maintenance 279

Figure 168 Load Factory Default: Start 280
Figure 169 Reboot System: Confirmation 281
Figure 170 Management > Maintenance > Firmware Upgrade 281
Figure 171 Management > Maintenance > Restore Configuration 282
Figure 172 Management > Maintenance > Backup Configuration 282
Figure 173 Management > Access Control 285
Figure 174 SNMP Management Model 286
Figure 175 Management > Access Control > SNMP 291
Figure 176 Management > Access Control > SNMP > Trap Group 293
Figure 177 Management > Access Control > Logins 294
Figure 178 SSH Communication Example 295
Figure 179 How SSH Works 295
Figure 180 HTTPS Implementation 297
Figure 181 Security Alert Dialog Box (Internet Explorer) 297
Figure 182 Security Certificate 1 (Netscape) 298
Figure 183 Security Certificate 2 (Netscape) 298
Figure 184 Example: Lock Denoting a Secure Connection 299
Figure 185 Management > Access Control > Service Access Control 299
Figure 186 Management > Access Control > Remote Management 300
Figure 187 Management > Diagnostic 303
Figure 188 Management > Syslog 306
Figure 189 Management > Syslog > Server Setup 307
Figure 190 Clustering Application Example 310
Figure 191 Management > Cluster Management 310
Figure 192 Cluster Management: Cluster Member Web Configurator Screen 311
Figure 193 Example: Uploading Firmware to a Cluster Member Switch 312
Figure 194 Management > Clustering Management > Configuration 313
Figure 195 MAC Table Flowchart 316
Figure 196 Management > MAC Table 316
Figure 197 IP Table Flowchart 317
Figure 198 Management > IP Table 318
Figure 199 Management > ARP Table 320
Figure 200 Management > Routing Table 321
Figure 201 Management > Configure Clone 323
Figure 202 Pop-up Blocker 328
Figure 203 Internet Options 329
Figure 204 Internet Options 330
Figure 205 Pop-up Blocker Settings 330
Figure 206 Internet Options 331
Figure 207 Security Settings - Java Scripting 332
Figure 208 Security Settings - Java 332
Figure 209 Java (Sun) 333
Figure 210 Network Number and Host ID 346

Figure 211 Subnetting Example: Before Subnetting 348
Figure 212 Subnetting Example: After Subnetting 349

List of Tables

Table 1 Panel Connections 43
Table 2 Panel Connections 46
Table 3 LEDs 47
Table 4 Navigation Panel Sub-links Overview 53
Table 5 Web Configurator Screen Sub-links Details 55
Table 6 Navigation Panel Links 56
Table 7 Status 68
Table 8 Status > Port Details 69
Table 9 Basic Setting > System Info 74
Table 10 Basic Setting > General Setup 75
Table 11 Basic Setting > Switch Setup 78
Table 12 Basic Setting > IP Setup 80
Table 13 Basic Setting > Port Setup 82
Table 14 IEEE 802.1Q VLAN Terminology 88
Table 15 Advanced Application > VLAN: VLAN Status 90
Table 16 Advanced Application > VLAN > VLAN Detail 91
Table 17 Advanced Application > VLAN > Static VLAN 92
Table 18 Advanced Application > VLAN > VLAN Port Setting 93
Table 19 Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN Setup 95
Table 20 Advanced Application > VLAN > VLAN Port Setting > Protocol Based VLAN Setup 98
Table 21 Advanced Application > VLAN: Port Based VLAN Setup 102
Table 22 Advanced Application > Static MAC Forwarding 104
Table 23 Advanced Application > FIltering 105
Table 24 STP Path Costs 108
Table 25 STP Port States 108
Table 26 Advanced Application > Spanning Tree Protocol > Configuration 113
Table 27 Advanced Application > Spanning Tree Protocol > RSTP 114
Table 28 Advanced Application > Spanning Tree Protocol > Status: RSTP 116
Table 29 Advanced Application > Spanning Tree Protocol > MRSTP 117
Table 30 Advanced Application > Spanning Tree Protocol > Status: MRSTP 119
Table 31 Advanced Application > Spanning Tree Protocol > MSTP 122
Table 32 Advanced Application > Spanning Tree Protocol > Status: MSTP 124
Table 33 Advanced Application > Bandwidth Control 128
Table 34 Advanced Application > Broadcast Storm Control 130
Table 35 Advanced Application > Mirroring 132
Table 36 Link Aggregation ID: Local Switch 134
Table 37 Link Aggregation ID: Peer Switch 134
Table 38 Advanced Application > Link Aggregation Status 134

Table 39 Advanced Application > Link Aggregation > Link Aggregation Setting 136
Table 40 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP 137
Table 41 Advanced Application > Port Authentication > 802.1x 144
Table 42 Advanced Application > Port Authentication > MAC Authentication 145
Table 43 Advanced Application > Port Security 148
Table 44 Advanced Application > Classifier 152
Table 45 Classifier: Summary Table 154
Table 46 Common Ethernet Types and Protocol Number 154
Table 47 Common IP Ports 155
Table 48 Advanced Application > Policy Rule 159
Table 49 Policy: Summary Table 160
Table 50 Advanced Application > Queuing Method 165
Table 51 VLAN Tag Format 169
Table 52 Single and Double Tagged 802.11Q Frame Format 169
Table 53 802.1Q Frame 169
Table 54 Advanced Application > VLAN Stacking 170
Table 55 Multicast Status 174
Table 56 Advanced Application > Multicast > Multicast Setting 175
Table 57 Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN 177
Table 58 Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile 179
Table 59 Advanced Application > Multicast > Multicast Setting > MVR 182
Table 60 Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration 184
Table 61 RADIUS vs TACACS+ 188
Table 62 Advanced Application > Auth and Acct > RADIUS Server Setup 189
Table 63 Advanced Application > Auth and Acct > TACACS+ Server Setup 191
Table 64 Advanced Application > Auth and Acct > Auth and Acct Setup 193
Table 65 Supported VSAs 195
Table 66 Supported Tunnel Protocol Attribute 196
Table 67 RADIUS Attributes - Exec Events via Console 198
Table 68 RADIUS Attributes - Exec Events via Telnet/SSH 198
Table 69 RADIUS Attributes - Exec Events via Console 198
Table 70 IP Source Guard 205
Table 71 IP Source Guard Static Binding 206
Table 72 DHCP Snooping 208
Table 73 DHCP Snooping Configure 210
Table 74 DHCP Snooping Port Configure 212
Table 75 DHCP Snooping VLAN Configure 213
Table 76 ARP Inspection Status 214
Table 77 ARP Inspection VLAN Status 215
Table 78 ARP Inspection Log Status 216
Table 79 ARP Inspection Configure 217
Table 80 ARP Inspection Port Configure 219
Table 81 ARP Inspection VLAN Configure 220

Table 82 Advanced Application > Loop Guard 223
Table 83 IP Application > Static Routing 227
Table 84 IP Application > RIP 230
Table 85 OSPF vs. RIP 231
Table 86 OSPF: Router Types 231
Table 87 IP Application > OSPF Status 234
Table 88 OSPF Status: Common Output Fields 234
Table 89 IP Application > OSPF Configuration: Activating and General Settings 236
Table 90 IP Application > OSPF Configuration: Area Setup 237
Table 91 IP Application > OSPF Configuration: Summary Table 238
Table 92 IP Application > OSPF Configuration > OSPF Interface 239
Table 93 IP Application > OSPF Configuration > OSPF Virtual Link 241
Table 94 IP Application > IGMP 246
Table 95 IP Application > DVMRP 249
Table 96 DVMRP: Default Timer Values 250
Table 97 IP Application > DiffServ 254
Table 98 IP Application > DiffServ > 2-rate 3 Color Marker 255
Table 99 Default DSCP-IEEE 802.1p Mapping 256
Table 100 IP Application > DiffServ > DSCP Setting 257
Table 101 IP Application > DHCP Status 260
Table 102 IP Application > DHCP Server Status Detail 261
Table 103 Relay Agent Information 262
Table 104 IP Application > DHCP > Global 262
Table 105 IP Application > DHCP > VLAN 265
Table 106 IP Application > VRRP Status 268
Table 107 IP Application > VRRP Configuration > IP Interface 269
Table 108 IP Application > VRRP Configuration > VRRP Parameters 271
Table 109 VRRP Configuring: VRRP Parameters 272
Table 110 Management > Maintenance 279
Table 111 Filename Conventions 283
Table 112 General Commands for GUI-based FTP Clients 284
Table 113 Access Control Overview 285
Table 114 SNMP Commands 286
Table 115 SNMP System Traps 287
Table 116 SNMP InterfaceTraps 288
Table 117 AAA Traps 289
Table 118 SNMP IP Traps 289
Table 119 SNMP Switch Traps 290
Table 120 Management > Access Control > SNMP 291
Table 121 Management > Access Control > SNMP > Trap Group 293
Table 122 Management > Access Control > Logins 294
Table 123 Management > Access Control > Service Access Control 300
Table 124 Management > Access Control > Remote Management 300

Table 125 Management > Diagnostic 303
Table 126 Syslog Severity Levels 305
Table 127 Management > Syslog 306
Table 128 Management > Syslog > Server Setup 307
Table 129 ZyXEL Clustering Management Specifications 309
Table 130 Management > Cluster Management 311
Table 131 FTP Upload to Cluster Member Example 312
Table 132 Management > Clustering Management > Configuration 313
Table 133 Management > MAC Table 316
Table 134 Management > IP Table 318
Table 135 Management > ARP Table 320
Table 136 Management > Routing Table 321
Table 137 Management > Configure Clone 324
Table 138 Troubleshooting the Start-Up of Your Switch 327
Table 139 Troubleshooting Accessing the Switch 327
Table 140 Troubleshooting the Password 333
Table 141 Hardware Specifications 335
Table 142 Firmware Specifications 336
Table 143 Switching Specifications 339
Table 144 Standards Supported 340
Table 145 IP Address Network Number and Host ID Example 346
Table 146 Subnet Masks 347
Table 147 Maximum Host Numbers 347
Table 148 Alternative Subnet Mask Notation 347
Table 149 Subnet 1 349
Table 150 Subnet 2 350
Table 151 Subnet 3 350
Table 152 Subnet 4 350
Table 153 Eight Subnets 350
Table 154 24-bit Network Number Subnet Planning 351
Table 155 16-bit Network Number Subnet Planning 351

PART I
Introduction

Getting to Know Your Switch (35)
Hardware Installation and Connection (39)
Hardware Overview (43)

1

Getting to Know Your Switch

This chapter introduces the main features and applications of the Switch.

1.1 Introduction

Your Switch is a stand-alone, layer-3, Gigabit Ethernet (GbE) switch with two 12 Gigabit stacking ports as well as support for an optional 2-port 10 Gigabit uplink module. By integrating router functions, the Switch performs wire-speed layer-3 routing in addition to layer-2 switching.

The XGS-4528F comes with 24 GbE dual personality interfaces. A dual personality interface includes one Gigabit port and one slot for a mini-GBIC transceiver (SFP module) with one port active at a time.

There are two XGS-4528F models. The XGS-4528F DC model requires DC power supply input of -36 VDC to -72 VDC, 1.5 A Max no tolerance. The XGS-4528F AC model requires 100 VAC to 240 VAC, 0.8 A power.

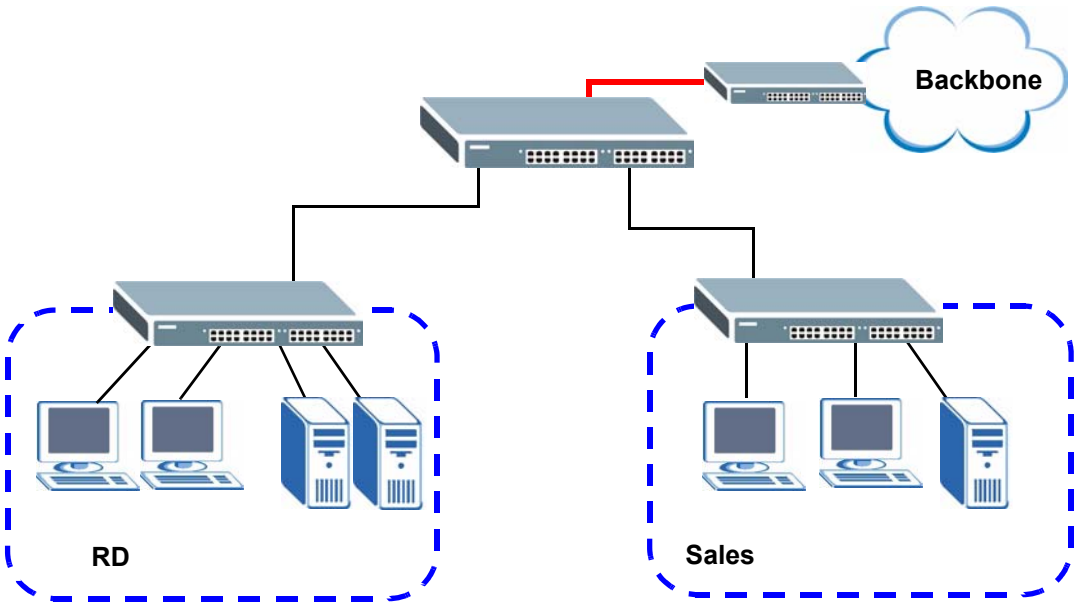
With its built-in web configurator, managing and configuring the Switch is easy. In addition, the Switch can also be managed via Telnet, any terminal emulator program on the console port, or third-party SNMP management.

See Chapter 45 on page 335 for a full list of software features available on the Switch.

1.1.1 Bridging Example

In this example the Switch connects different company departments (**RD** and **Sales**) to the corporate backbone. It can alleviate bandwidth contention and eliminate server and network bottlenecks. All users that need high bandwidth can connect to high-speed department servers via the Switch. You can provide a super-fast uplink connection by using the optional 10 Gigabit uplink module on the Switch.

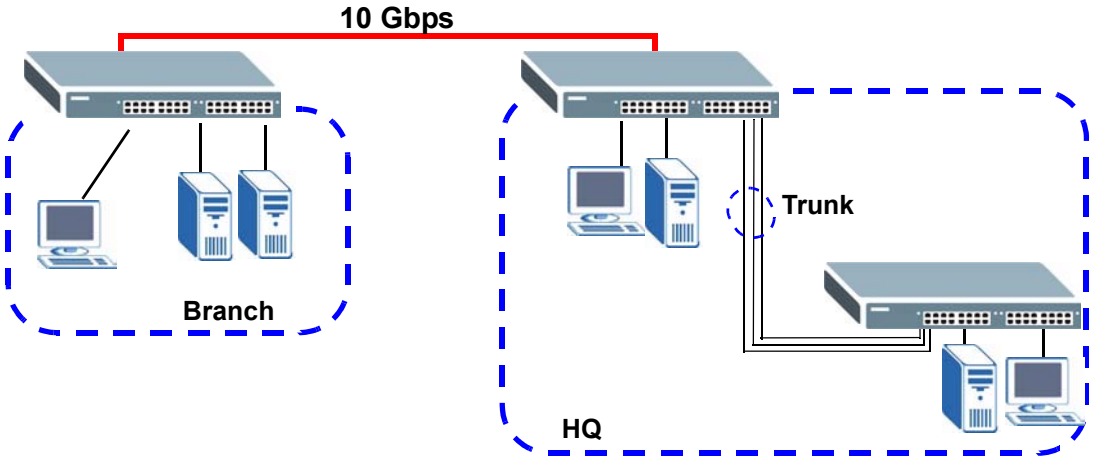
Figure 1 Bridging Application



1.1.2 High Performance Switching Example

The Switch is ideal for connecting two geographically dispersed networks that need high bandwidth. In the following example, a company uses the optional 10 Gigabit uplink modules to connect the headquarters to a branch office network. Within the headquarters network, a company can use trunking to group several physical ports into one logical higher-capacity link. Trunking can be used if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.

Figure 2 High Performance Switching

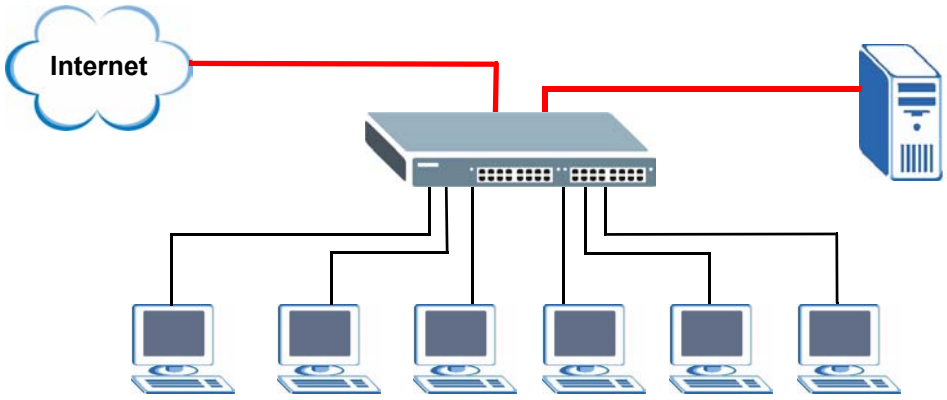


1.1.3 Gigabit Ethernet to the Desktop

The Switch is an ideal solution for small networks which demand high bandwidth for a group of heavy traffic users. You can connect computers and servers directly to the Switch's port or connect other switches to the Switch. Use the optional 10 Gigabit uplink module to provide high speed access to a data server and the Internet. The uplink module supports a fiber-optic connection which alleviates the distance limitations of copper cabling.

In this example, all computers can share high-speed applications on the server and access the Internet. To expand the network, simply add more networking devices such as switches, routers, computers, print servers and so on.

Figure 3 Gigabit to the Desktop



1.1.4 IEEE 802.1Q VLAN Application Example

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one or more groups. With VLAN, a station cannot directly talk to or hear from stations that are not in the same group(s) unless such traffic first goes through a router.

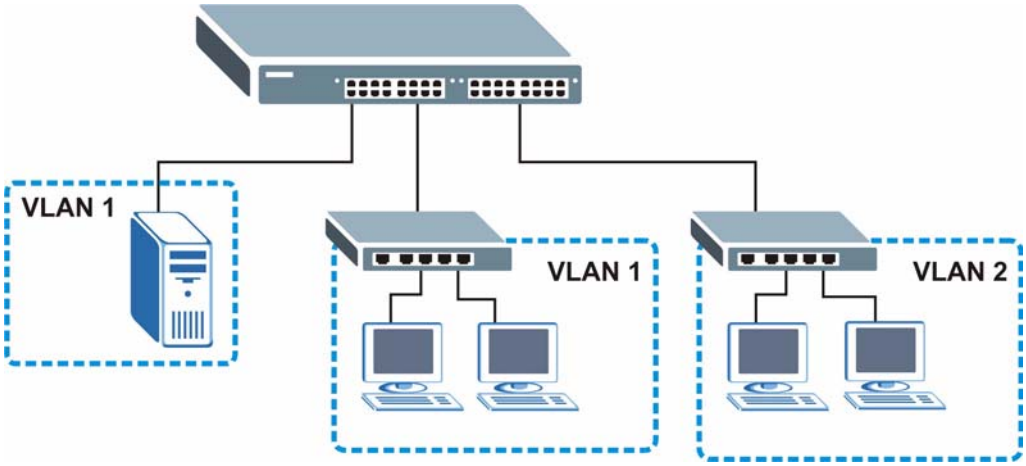
For more information on VLANs, refer to Chapter 8 on page 87.

1.1.4.1 Tag-based VLAN Example

Ports in the same VLAN group share the same frame broadcast domain, thus increasing network performance by reducing broadcast traffic. VLAN groups can be modified at any time by adding, moving or changing ports without any re-cabling.

Shared resources such as a server can be used by all ports in the same VLAN as the server. In the following figure only ports that need access to the server need to be part of VLAN 1. Ports can belong to other VLAN groups too.

Figure 4 Shared Server Using VLAN Example



1.2 Ways to Manage the Switch

Use any of the following methods to manage the Switch.

- Web Configurator. This is recommended for everyday management of the Switch using a (supported) web browser. See Chapter 4 on page 51.
- Command Line Interface. Line commands offer an alternative to the Web Configurator and may be necessary to configure advanced features. See the CLI Reference Guide.
- FTP. Use File Transfer Protocol for firmware upgrades and configuration backup/restore. See Section 34.8 on page 283.
- SNMP. The device can be monitored and/or managed by an SNMP manager. See Section 35.3 on page 286.

1.3 Good Habits for Managing the Switch

Do the following things regularly to make the Switch more secure and to manage the Switch more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the Switch to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the Switch. You could simply restore your last configuration.

2

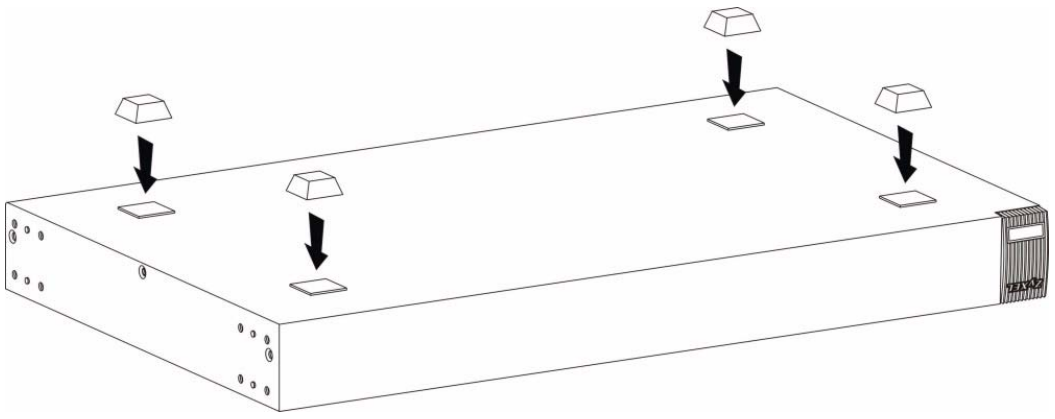
Hardware Installation and Connection

This chapter shows you how to install and connect the Switch.

2.1 Freestanding Installation

1. Make sure the Switch is clean and dry.
2. Set the Switch on a smooth, level surface strong enough to support the weight of the Switch and the connected cables. Make sure there is a power outlet nearby.
3. Make sure there is enough clearance around the Switch to allow air circulation and the attachment of cables and the power cord.
4. Remove the adhesive backing from the rubber feet.
5. Attach the rubber feet to each corner on the bottom of the Switch. These rubber feet help protect the Switch from shock or vibration and ensure space between devices when stacking.

Figure 5 Attaching Rubber Feet



Do NOT block the ventilation holes. Leave space between devices when stacking.

For proper ventilation, allow at least 4 inches (10 cm) of clearance at the front and 3.4 inches (8 cm) at the back of the Switch. This is especially important for enclosed rack installations.

2.2 Mounting the Switch on a Rack

This section lists the rack mounting requirements and precautions and describes the installation steps.

2.2.1 Rack-mounted Installation Requirements

- Two mounting brackets.
- Eight M3 flat head screws and a #2 Philips screwdriver.
- Four M5 flat head screws and a #2 Philips screwdriver.

Failure to use the proper screws may damage the unit.

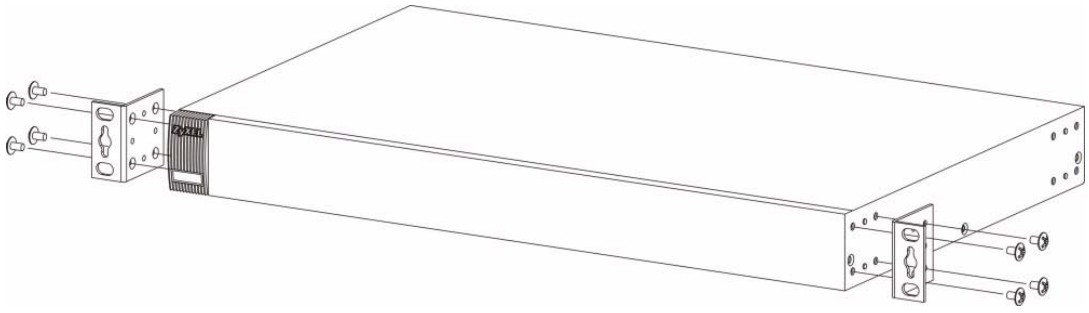
2.2.1.1 Precautions

- Make sure the rack will safely support the combined weight of all the equipment it contains.
- Make sure the position of the Switch does not make the rack unstable or top-heavy. Take all necessary precautions to anchor the rack securely before installing the unit.

2.2.2 Attaching the Mounting Brackets to the Switch

1 Position a mounting bracket on one side of the Switch, lining up the four screw holes on the bracket with the screw holes on the side of the Switch.

Figure 6 Attaching the Mounting Brackets



2 Using a #2 Philips screwdriver, install the M3 flat head screws through the mounting bracket holes into the Switch.

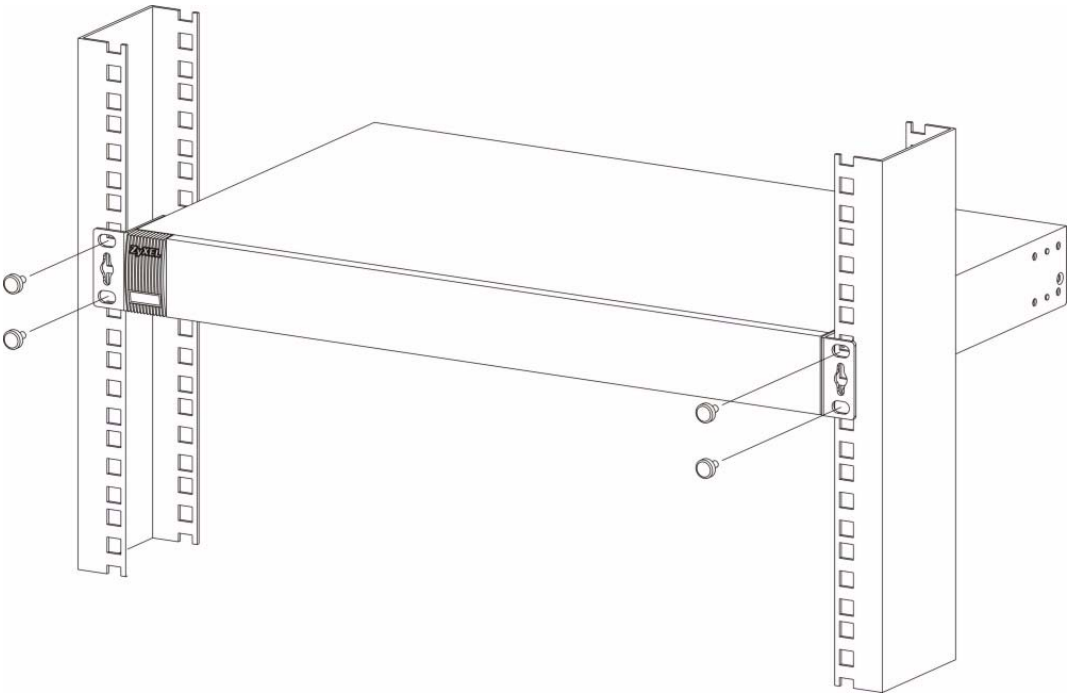
3 Repeat steps 1 and 2 to install the second mounting bracket on the other side of the Switch.

4 You may now mount the Switch on a rack. Proceed to the next section.

2.2.3 Mounting the Switch on a Rack

1 Position a mounting bracket (that is already attached to the Switch) on one side of the rack, lining up the two screw holes on the bracket with the screw holes on the side of the rack.

Figure 7 Mounting the Switch on a Rack



2 Using a #2 Philips screwdriver, install the M5 flat head screws through the mounting bracket holes into the rack.

3 Repeat steps 1 and 2 to attach the second mounting bracket on the other side of the rack.

3

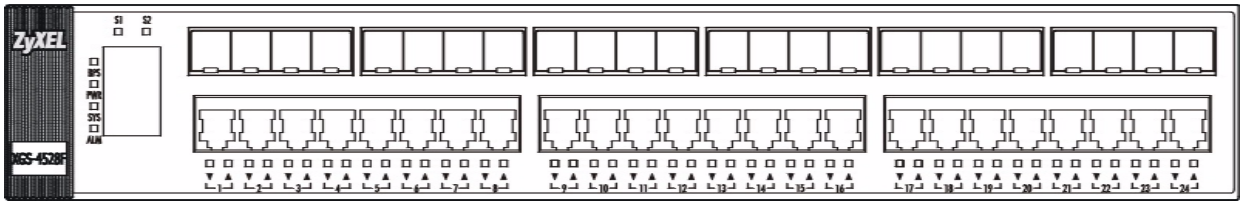
Hardware Overview

This chapter describes the front panel and rear panel of the Switch and shows you how to make the hardware connections.

3.1 Front Panel Connections

The figure below shows the front panel of the Switch.

Figure 8 Front Panel



The following table describes the ports.

Table 1 Panel Connections

CONNECTOR	DESCRIPTION
24 Dual Personality Interfaces	Each interface has one 1000Base-T copper RJ-45 port and one mini-GBIC (Gigabit Interface Converter) fiber port, with one port active at a time.
	• 24 1000Base-T Ports: Connect these ports to high-bandwidth backbone network Ethernet switches using Category 5/5e/6 1000Base-T Ethernet cables.
	• 24 Mini-GBIC Ports: Use Small Form-Factor Pluggable (SFP) transceivers in these ports for 1000Base-X fiber-optic connections to backbone Ethernet switches.

3.1.1 Dual Personality Interfaces

There are 24 Dual Personality interfaces, comprising 24 1000Base-T/mini-GBIC combo ports. For each interface you can connect either to the 1000Base-T port or the mini-GBIC port. The mini-GBIC ports have priority over the 1000Base-T ports. This means that if a mini-GBIC port and the corresponding 1000Base-T port are connected at the same time, the 1000Base-T port will be disabled.

3.1.2 1000Base-T Ports

The Switch has 24 1000Base-T auto-negotiating, auto-crossover Ethernet ports. In 100/1000 Mbps Gigabit Ethernet, the speed can be 100 Mbps or 1000 Mbps. The duplex mode can be both half or full duplex at 100 Mbps and full duplex only at 1000 Mbps.

An auto-negotiating port can detect and adjust to the optimum Ethernet speed (100/1000 Mbps) and duplex mode (full duplex or half duplex) of the connected device.

An auto-crossover (auto-MDI/MDI-X) port automatically works with a straight-through or crossover Ethernet cable.

3.1.2.1 Default Ethernet Settings

The factory default negotiation settings for the Ethernet ports on the Switch are:

- Speed: Auto
- Duplex: Auto
- Flow control: Off

3.1.3 Mini-GBIC Slots

These are 24 slots for Small Form-Factor Pluggable (SFP) transceivers. A transceiver is a single unit that houses a transmitter and a receiver. Use a transceiver to connect a fiber-optic cable to the Switch. The Switch does not come with transceivers. You must use transceivers that comply with the Small Form-Factor Pluggable (SFP) Transceiver MultiSource Agreement (MSA). See the SFF committee's INF-8074i specification Rev 1.0 for details.

You can change transceivers while the Switch is operating. You can use different transceivers to connect to Ethernet switches with different types of fiber-optic connectors.

- Type: SFP connection interface
- Connection speed: 1 Gigabit per second (Gbps)

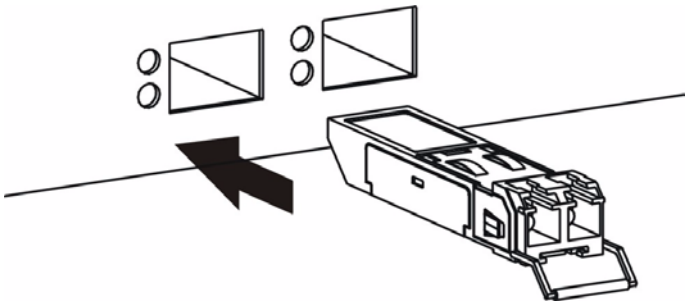
To avoid possible eye injury, do not look into an operating fiber-optic module's connectors.

3.1.3.1 Transceiver Installation

Use the following steps to install a mini GBIC transceiver (SFP or XFP module).

1 Insert the transceiver into the slot with the exposed section of PCB board facing down.

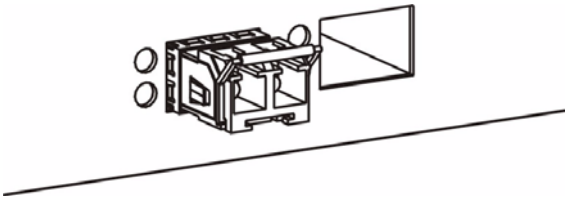
Figure 9 Transceiver Installation Example



2 Press the transceiver firmly until it clicks into place.

3 The Switch automatically detects the installed transceiver. Check the LEDs to verify that it is functioning properly.

Figure 10 Installed Transceiver

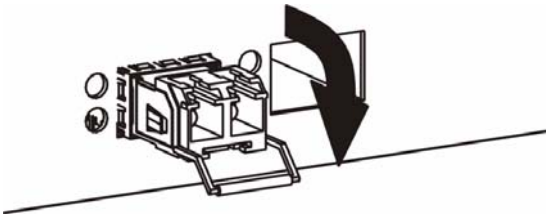


3.1.3.2 Transceiver Removal

Use the following steps to remove a mini GBIC transceiver (SFP module).

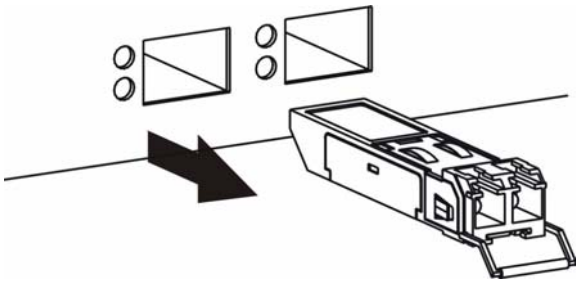
1 Open the transceiver's latch (latch styles vary).

Figure 11 Opening the Transceiver's Latch Example



2 Pull the transceiver out of the slot.

Figure 12 Transceiver Removal Example



3.2 Rear Panel

The following figures show the rear panels of the AC and DC power input model switches. The rear panels contain:

- A connector for the backup power supply (**A**)
- An optional uplink module (**B**)
- Two stacking ports (**C**)
- An RJ-45 out-of-band management port (**D**)
- An RS-232 management console port (**E**)
- A connector for the power receptacle (**F**)
- A power switch (**G**) (DC power input model only).

Figure 13 Rear Panel - AC Model

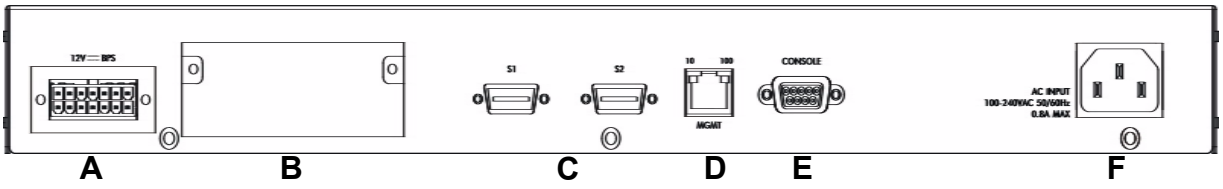
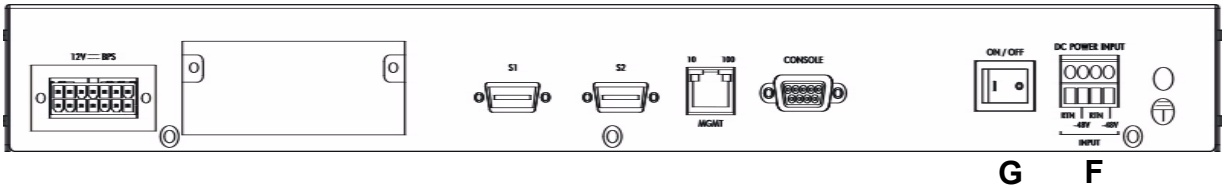


Figure 14 Rear Panel - DC Model



The following table describes the ports on the rear panel.

Table 2 Panel Connections

CONNECTOR	DESCRIPTION
Optional two 10 GbE Ports	These ports are part of the optional uplink module which you can use to connect your switch to other high-speed Ethernet switches in your network. Use 10 Gigabit Small Form Factor Pluggable (XFP) transceivers to connect 1000Base-X fiber-optic cables to these ports. See Section 3.1.3.1 on page 44 and Section 3.1.3.2 on page 45 for information on installing and removing transceivers. See the EM-422 User's Guide for more information on this module.
Two stacking ports	Connect these ports to other XGS-4528F switches for stacking using stacking cables.
Management Port	Connect to a computer using an RJ-45 Ethernet cable for local configuration of the Switch.
Console Port	Only connect this port to your computer (using an RS-232 cable) if you want to configure the Switch using the command line interface (CLI) via the console port.

3.2.1 Power Connector

Make sure you are using the correct power source as shown on the panel.

To connect the power to the Switch, insert the female end of power cord to the power receptacle on the rear panel. Connect the other end of the supplied power cord to a power outlet. Make sure that no objects obstruct the airflow of the fans.

The Switch's AC unit requires a power supply of 100~240 VAC, 0.8 A.

The Switch's DC version requires a power supply of -48 VDC to -60 VDC, 2.3 A max, no tolerance.

3.2.2 External Backup Power Supply Connector

The Switch supports external backup power supply (BPS).

The Switch constantly monitors the status of the internal power supply. The backup power supply automatically provides power to the Switch in the event of a power failure. Once the Switch receives power from the backup power supply, it will not automatically switch back to using the internal power supply even when the power is resumed.

3.2.3 Console Port

For local management, you can use a computer with terminal emulation software configured to the following parameters:

- VT100 terminal emulation
- 9600 bps
- No parity, 8 data bits, 1 stop bit
- No flow control

Connect the male 9-pin end of the RS-232 console cable to the console port of the Switch. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer.

3.3 LEDs

The following table describes the LEDs.

Table 3 LEDs

LED	COLOR	STATUS	DESCRIPTION
BPS	Green	Blinking	The system is receiving power from the backup power supply.
		On	The backup power supply is connected and active.
		Off	The backup power supply is not ready or not active.
PWR	Green	On	The system is turned on.
		Off	The system is off.
SYS	Green	Blinking	The system is rebooting and performing self-diagnostic tests.
		On	The system is on and functioning properly.
		Off	The power is off or the system is not ready/malfunctioning.

Table 3 LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
ALM	Red	On	There is a hardware failure.
		Off	The system is functioning normally.
S1	Green	On	The Switch is connected to other switches in the stack on Stacking Port 1.
		Off	The Switch is not connected to other switches in the stack on Stacking Port 1.
S2	Green	On	The Switch is connected to other switches in the stack on Stacking Port 2.
		Off	The Switch is not connected to other switches in the stack on Stacking Port 2.
System Status		Displays hourglass icon	The Switch is starting up.
		Displays Stack ID number	The LED is showing the Stack ID number of the Switch.
1000Base-T Gigabit Ports (▼)			
1-24	Green	Blinking	The system is transmitting/receiving to/from a 10/1000 Mbps Ethernet network.
		On	The link to a 10/1000 Mbps Ethernet network is up.
	Amber	Blinking	The system is transmitting/receiving to/from a 100 Mbps Ethernet network.
		On	The link to a 100 Mbps Ethernet network is up.
		Off	The link to an Ethernet network is down.
1000Base-X Mini-GBIC Slots (▲)			
1-24	Green	On	The port has a successful connection.
		Blinking	The port is receiving or transmitting data.
		Off	This link is disconnected.

PART II
Basic Configuration

The Web Configurator (51)
Initial Setup Example (61)
System Status and Port Statistics (67)
Basic Setting (73)

4

The Web Configurator

This section introduces the configuration and functions of the web configurator.

4.1 Introduction

The web configurator is an HTML-based management interface that allows easy Switch setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

4.2 System Login

1. Start your web browser.
2. Type “http://” and the IP address of the Switch (for example, the default is 192.168.1.1) in the Location or Address field. Press [ENTER].
3. The login screen appears. The default username is **admin** and associated default password is **1234**. The date and time display as shown if you have not configured a time server nor manually entered a time and date in the **General Setup** screen.

Figure 15 Web Configurator: Login

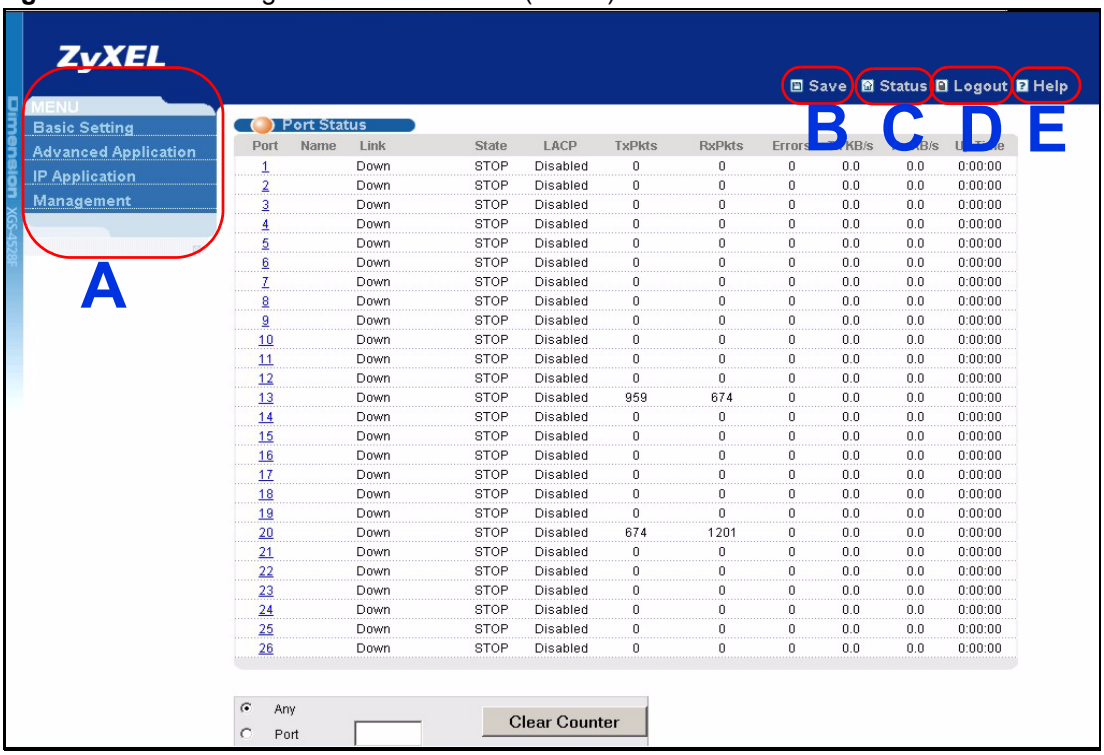
4 Click **OK** to view the first web configurator screen.

4.3 The Status Screen

The **Status** screen is the first screen that displays when you access the web configurator.

The following figure shows the navigating components of a web configurator screen.

Figure 16 Web Configurator Home Screen (Status)



A - Click the menu items to open submenu links, and then click on a submenu link to open the screen in the main window.

B, C, D, E - These are quick links which allow you to perform certain tasks no matter which screen you are currently working in.

B - Click this link to save your configuration into the Switch's nonvolatile memory. Nonvolatile memory is saved in the configuration file from which the Switch booted from and it stays the same even if the Switch's power is turned off. See Section 34.3 on page 280 for information on saving your settings to a specific configuration file.

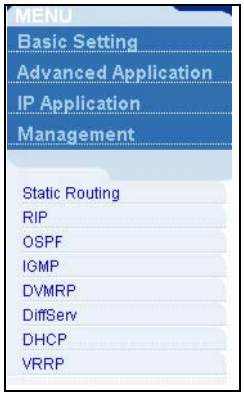
C - Click this link to go to the status page of the Switch.

D - Click this link to log out of the web configurator.

E - Click this link to display web help pages. The help pages provide descriptions for all of the configuration screens.

In the navigation panel, click a main link to reveal a list of submenu links.

Table 4 Navigation Panel Sub-links Overview

BASIC SETTING	ADVANCED APPLICATION	IP APPLICATION	MANAGEMENT
			

The following table lists the various web configurator screens within the sub-links.

Table 5 Web Configurator Screen Sub-links Details

BASIC SETTING	ADVANCED APPLICATION	IP APPLICATION	MANAGEMENT
System Info General Setup Switch Setup IP Setup Port Setup	VLAN (Status) VLAN Port Setting - Subnet Based VLAN - Protocol Based VLAN Static VLAN Static MAC Forwarding Filtering Spanning Tree Protocol (Status) Configuration RSTP MRSTP MSTP Bandwidth Control Broadcast Storm Control Mirroring Link Aggregation (Status) Link Aggregation Setting - Link Aggregation Control Protocol Port Authentication 802.1x MAC Authentication Port Security Classifier Policy Rule Queuing Method VLAN Stacking Multicast (Status) Multicast Setting - IGMP Snooping VLAN - IGMP Filtering Profile - MVR -- Group Configuration Authentication and Accounting RADIUS Server Setup TACACS+ Server Setup Auth and Acct Setup IP Source Guard IP Source Guard Static Binding DHCP Snooping - DHCP Snooping Configure -- DHCP Snooping Port Configure -- DHCP Snooping VLAN Configure ARP Inspection Status - ARP Inspection VLAN Status - ARP Inspection Log Status - ARP Inspection Configure -- ARP Inspection Port Configure -- ARP Inspection VLAN Configure Loop Guard	Static Routing RIP OSPF (Status) OSPF Configuration - OSPF Interface - OSPF Virtual-Link IGMP DVMRP DiffServ 2-Rate 3 Color Marker DSCP Setting DHCP (Status) DHCP Relay VLAN Setting VRRP (Status) VRRP Configuration	Maintenance Firmware Upgrade Restore Configuration Backup Configuration Access Control SNMP - Trap Group Logins Service Access Control Remote Management Diagnostic Syslog (Setup) Syslog Server Setup Cluster Management (Status) Configuration MAC Table IP Table ARP Table Routing Table (Status) Configure Clone

The following table describes the links in the navigation panel.

Table 6 Navigation Panel Links

LINK	DESCRIPTION
Basic Settings	
System Info	This link takes you to a screen that displays general system and hardware monitoring information.
General Setup	This link takes you to a screen where you can configure general identification information and time settings for the Switch.
Switch Setup	This link takes you to a screen where you can set up global Switch parameters such as VLAN type, MAC address learning, IGMP snooping, GARP and priority queues.
IP Setup	This link takes you to a screen where you can configure the IP address, subnet mask (necessary for Switch management) and DNS (domain name server) and set up to 64 IP routing domains.
Port Setup	This link takes you to screens where you can configure speed, flow control and priority settings for individual Switch ports.
Advanced Application	
VLAN	This link takes you to screens where you can configure port-based or 802.1Q VLAN (depending on what you configured in the Switch Setup menu). You can also configure a protocol based VLAN or a subnet based VLAN in these screens.
Static MAC Forwarding	This link takes you to screens where you can configure static MAC addresses for a port. These static MAC addresses do not age out.
Filtering	This link takes you to a screen to set up filtering rules.
Spanning Tree Protocol	This link takes you to screens where you can configure the RSTP/MRSTP/MSTP to prevent network loops.
Bandwidth Control	This link takes you to screens where you can cap the maximum bandwidth allowed from specified source(s) to specified destination(s).
Broadcast Storm Control	This link takes you to a screen to set up broadcast filters.
Mirroring	This link takes you to screens where you can copy traffic from one port or ports to another port in order that you can examine the traffic from the first port without interference.
Link Aggregation	This link takes you to screen where you can logically aggregate physical links to form one logical, higher-bandwidth link.
Port Authentication	This link takes you to a screen where you can configure IEEE 802.1x port authentication as well as MAC authentication for clients communicating via the Switch.
Port Security	This link takes you to a screen where you can activate MAC address learning and set the maximum number of MAC addresses to learn on a port.
Classifier	This link takes you to a screen where you can configure the Switch to group packets based on the specified criteria.
Policy Rule	This link takes you to a screen where you can configure the Switch to perform special treatment on the grouped packets.
Queuing Method	This link takes you to a screen where you can configure queuing with associated queue weights for each port.
VLAN Stacking	This link takes you to a screen where you can activate and configure VLAN stacking.
Multicast	This link takes you to screen where you can configure various multicast features and create multicast VLANs.

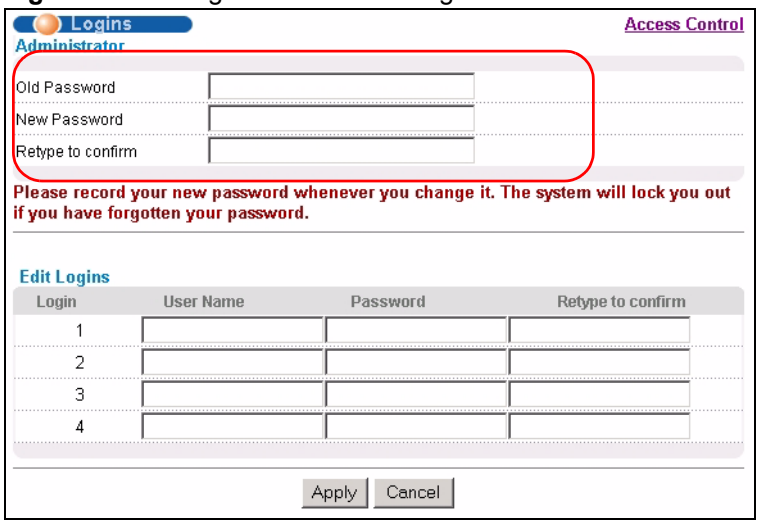
Table 6 Navigation Panel Links (continued)

LINK	DESCRIPTION
Auth and Acct	This link takes you to screens where you can configure authentication and accounting services via external servers. The external servers can be either RADIUS (Remote Authentication Dial-In User Service) or TACACS+ (Terminal Access Controller Access-Control System Plus).
IP Source Guard	This link takes you to screens where you can configure filtering of unauthorized DHCP and ARP packets in your network.
Loop Guard	This link takes you to a screen where you can configure protection against network loops that occur on the edge of your network.
IP Application	
Static Route	This link takes you to a screen where you can configure static routes. A static route defines how the Switch should forward traffic by configuring the TCP/IP parameters manually.
RIP	This link takes you to a screen where you can configure the RIP (Routing Information Protocol) direction and versions.
OSPF	This link takes you to screens where you can view the OSPF status and configure OSPF settings.
IGMP	This link takes you to a screen where you can configure the IGMP settings.
DVMRP	This link takes you to a screen where you can configure the DVMRP (Distance Vector Multicast Routing Protocol) settings.
DiffServ	This link takes you to screens where you can enable DiffServ, configure marking rules and set DSCP-to-IEEE802.1p mappings.
DHCP	This link takes you to screens where you can configure the DHCP settings.
VRRP	This link takes you to screens where you can configure redundant virtual router for your network.
Management	
Maintenance	This link takes you to screens where you can perform firmware and configuration file maintenance as well as reboot the system.
Access Control	This link takes you to screens where you can change the system login password and configure SNMP and remote management.
Diagnostic	This link takes you to screens where you can view system logs and can test port(s).
Syslog	This link takes you to screens where you can setup system logs and a system log server.
Cluster Management	This link takes you to a screen where you can configure clustering management and view its status.
MAC Table	This link takes you to a screen where you can view the MAC address and VLAN ID of a device attach to a port. You can also view what kind of device it is.
IP Table	This link takes you to a screen where you can view the IP addresses and VLAN ID of a device attached to a port.You can also view what kind of device it is.
ARP Table	This link takes you to a screen where you can view the MAC address – IP address resolution table.
Routing Table	This link takes you to a screen where you can view the routing table.
Configure Clone	This link takes you to a screen where you can copy attributes of one port to (an)other port(s).

4.3.1 Change Your Password

After you log in for the first time, it is recommended you change the default administrator password. Click **Management** > **Access Control > Logins** to display the next screen.

Figure 17 Change Administrator Login Password



4.4 Saving Your Configuration

When you are done modifying the settings in a screen, click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

Click the **Save** link in the upper right hand corner of the web configurator to save your configuration to nonvolatile memory. Nonvolatile memory refers to the Switch's storage that remains even if the Switch's power is turned off.

Use the **Save** link when you are done with a configuration session.

4.5 Switch Lockout

You could block yourself (and all others) from using in-band-management (managing through the data ports) if you do one of the following:

1. Delete the management VLAN (default is VLAN 1).
2. Delete all port-based VLANs with the CPU port as a member. The "CPU port" is the management port of the Switch.
3. Filter all traffic to the CPU port.
4. Disable all ports.
5. Misconfigure the text configuration file.

6 Forget the password and/or IP address.
7 Prevent all services from accessing the Switch.
8 Change a service port number but forget it.

Be careful not to lock yourself and others out of the Switch. If you do lock yourself out, try using out-of-band management (via the management port) to configure the Switch.

4.6 Resetting the Switch

If you lock yourself (and others) from the Switch or forget the administrator password, you will need to reload the factory-default configuration file or reset the Switch back to the factory defaults.

4.6.1 Reload the Configuration File

Uploading the factory-default configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all previous configurations and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will also be reset to "1234" and the IP address to 192.168.1.1.

To upload the configuration file, do the following:

1 Connect to the console port using a computer with terminal emulation software. See Section 3.2 on page 46 for details.
2 Disconnect and reconnect the Switch's power to begin a session. When you reconnect the Switch's power, you will see the initial screen.
3 When you see the message "`Press any key to enter Debug Mode within 3 seconds ...`" press any key to enter debug mode.
4 Type `atlc` after the "`Enter Debug Mode`" message.
5 Wait for the "`Starting XMODEM upload`" message before activating XMODEM upload on your terminal.
6 After a configuration file upload, type `atgo` to restart the Switch.

Figure 18 Resetting the Switch: Via the Console Port

```
Bootbase Version: V1.00 | 01/23/2007 11:56:33
RAM:Size = 64 Mbytes
DRAM POST: Testing: 65536K OK
DRAM Test SUCCESS !
FLASH: Intel 32M

ZyNOS Version: V3.80(ARC.0)b4 | 07/04/2007 19:06:37

Press any key to enter debug mode within 3 seconds.....................
Enter Debug Mode
ras> atlc
Starting XMODEM upload (CRC mode)....
CCCCCCCCCCCCCCCC
Total  393216 bytes received.
Erasing..
............................................................
OK
ras> atgo
```

The Switch is now reinitialized with a default configuration file including the default password of “1234”.

4.7 Logging Out of the Web Configurator

Click **Logout** in a screen to exit the web configurator. You have to log in with your password again after you log out. This is recommended after you finish a management session for security reasons.

Figure 19 Web Configurator: Logout Screen

4.8 Help

The web configurator’s online help has descriptions of individual screens and some supplementary information.

Click the **Help** link from a web configurator screen to view an online help description of that screen.

5

Initial Setup Example

This chapter shows how to set up the Switch for an example network.

5.1 Overview

The following lists the configuration steps for the example network:

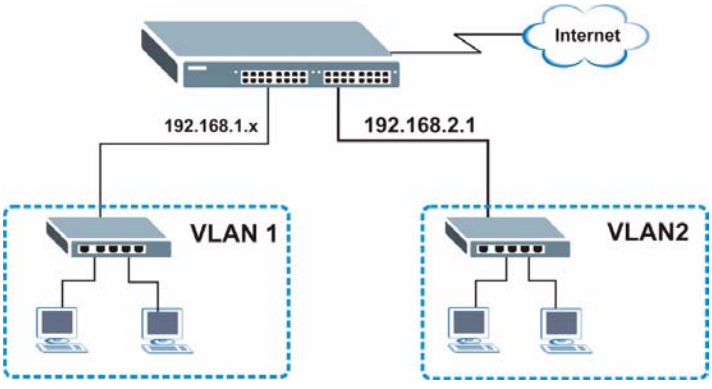
- Configure an IP interface
- Configure DHCP server settings
- Create a VLAN
- Set port VLAN ID
- Enable RIP

5.1.1 Configuring an IP Interface

On a layer-3 switch, an IP interface (also known as an IP routing domain) is not bound to a physical port. The default IP address of the Switch is 192.168.1.1 with a subnet mask of 255.255.255.0.

In the example network, since the **RD** network is already in the same IP interface as the Switch, you don't need to create an IP interface for it. However, if you want to have the **Sales** network on a different routing domain, you need to create a new IP interface. This allows the Switch to route traffic between the **RD** and **Sales** networks.

Figure 20 Initial Setup Network Example: IP Interface



1 Connect your computer to the **MGMT** port that is used only for management. Make sure your computer is in the same subnet as the **MGMT** port.

2 Open your web browser and enter 192.168.0.1 (the default **MGMT** port IP address) in the address bar to access the web configurator. See Section 4.2 on page 51 for more information.

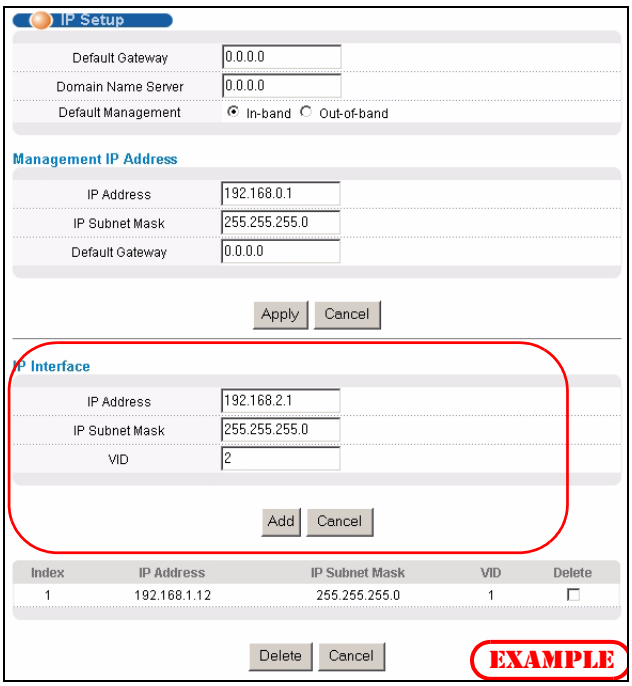
3 Click **Basic Setting** and **IP Setup** in the navigation panel.

4 Configure the related fields in the **IP Setup** screen.

For the **Sales** network, enter 192.168.2.1 as the IP address and 255.255.255.0 as the subnet mask.

5 In the **VID** field, enter the ID of the VLAN group to which you want this IP interface to belong. This is the same as the VLAN ID you configure in the **Static VLAN** screen.

6 Click **Add** to save the settings to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.



5.1.2 Configuring DHCP Server Settings

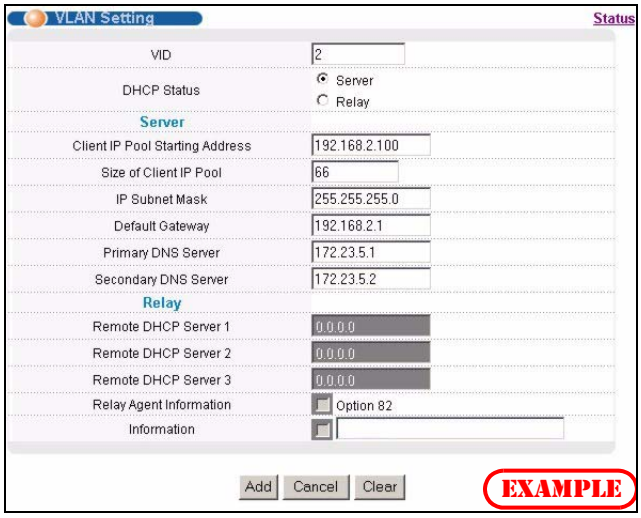
You can set the Switch to assign network information (such as the IP address, DNS server, etc.) to DHCP clients on the network.

For the example network, configure two DHCP client pools on the Switch for the DHCP clients in the **RD** and **Sales** networks.

1 In the web configurator, click **IP Application** and **DHCP** in the navigation panel and click the **VLAN** link.

2 In the **VLAN Setting** screen, specify the ID of the VLAN to which the DHCP clients belong, the starting IP address pool, subnet mask, default gateway address and the DNS server address(es).

3 Click **Add** to save the settings to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

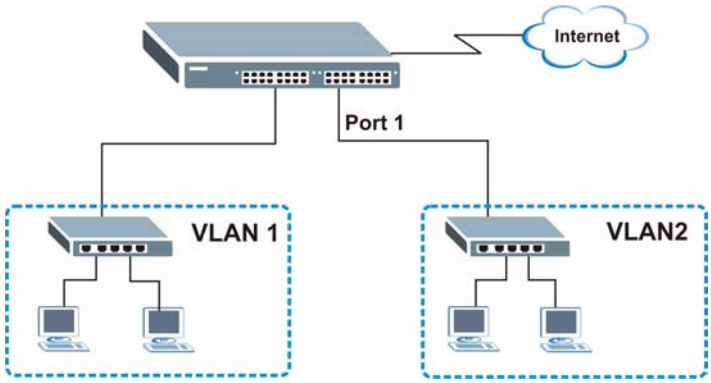


5.1.3 Creating a VLAN

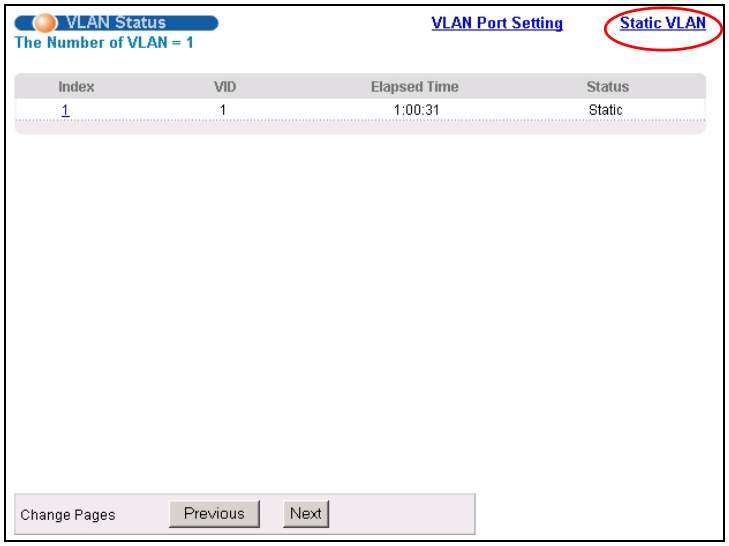
VLANs confine broadcast frames to the VLAN group in which the port(s) belongs. You can do this with port-based VLAN or tagged static VLAN with fixed port members.

In this example, you want to configure port 1 as a member of VLAN 2.

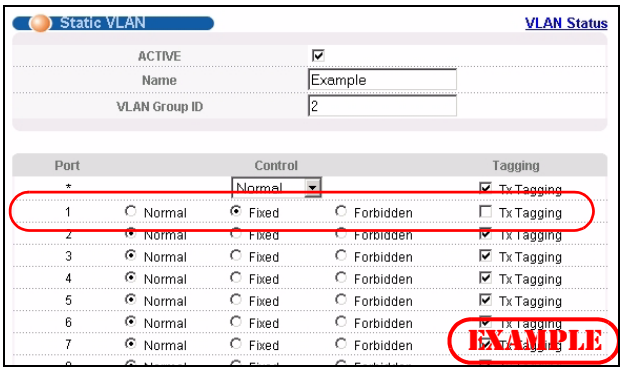
Figure 21 Initial Setup Network Example: VLAN



1 Click **Advanced Application** > **VLAN** in the navigation panel and click the **Static VLAN** link.



2 In the **Static VLAN** screen, select **ACTIVE**, enter a descriptive name in the **Name** field and enter 2 in the **VLAN Group ID** field for the **VLAN2** network.



The **VLAN Group ID** field in this screen and the **VID** field in the **IP Setup** screen refer to the same VLAN ID.

3 Since the **VLAN2** network is connected to port 1 on the Switch, select **Fixed** to configure port 1 to be a permanent member of the VLAN only.

4 To ensure that VLAN-unaware devices (such as computers and hubs) can receive frames properly, clear the **TX Tagging** check box to set the Switch to remove VLAN tags before sending.

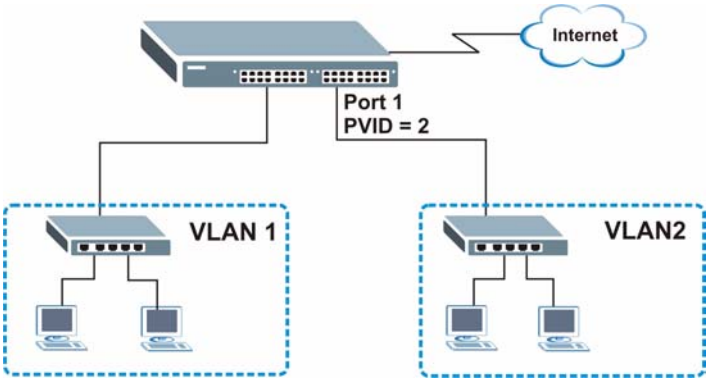
5 Click **Add** to save the settings to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

5.1.4 Setting Port VID

Use PVID to add a tag to incoming untagged frames received on that port so that the frames are forwarded to the VLAN group that the tag defines.

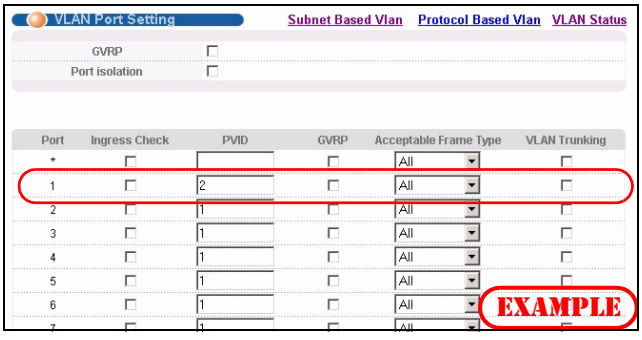
In the example network, configure 2 as the port VID on port 1 so that any untagged frames received on that port get sent to VLAN 2.

Figure 22 Initial Setup Network Example: Port VID



1 Click **Advanced Applications** and **VLAN** in the navigation panel. Then click the **VLAN Port Setting** link.

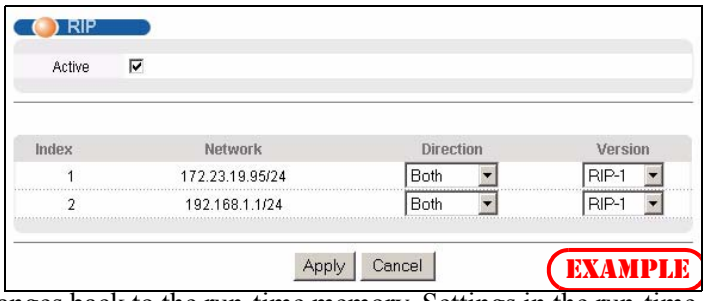
2 Enter 2 in the **PVID** field for port 1 and click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.



5.1.5 Enabling RIP

To exchange routing information with other routing devices across different routing domains, enable RIP (Routing Information Protocol) in the **RIP** screen.

1. Click **IP Application** and **RIP** in the navigation panel.
2. Select **Both** in the **Direction** field to set the Switch to broadcast and receive routing information.
3. In the **Version** field, select **RIP-1** for the RIP packet format that is universally supported.



4. Click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

6

System Status and Port Statistics

This chapter describes the system status (web configurator home page) and port details screens.

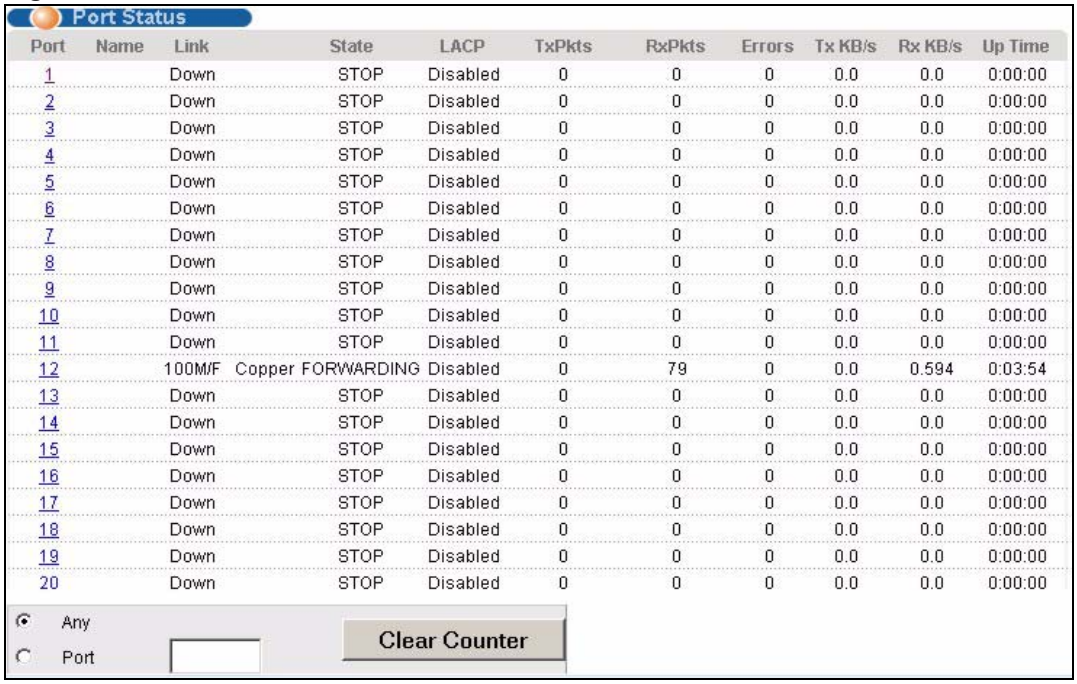
6.1 Overview

The home screen of the web configurator displays a port statistical summary with links to each port showing statistical details.

6.2 Port Status Summary

To view the port statistics, click **Status** in all web configurator screens to display the **Status** screen as shown next.

Figure 23 Status


Port Status
Port Name Link State LACP TxPkts RxPkts Errors Tx KB/s Rx KB/s Up Time
1 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
2 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
3 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
4 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
5 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
6 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
7 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
8 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
9 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
10 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
11 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
12 100M/F Copper FORWARDING Disabled 0 79 0 0.0 0.594 0:03:54
13 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
14 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
15 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
16 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
17 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
18 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
19 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
20 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
Any
Port
Clear Counter

The following table describes the labels in this screen.

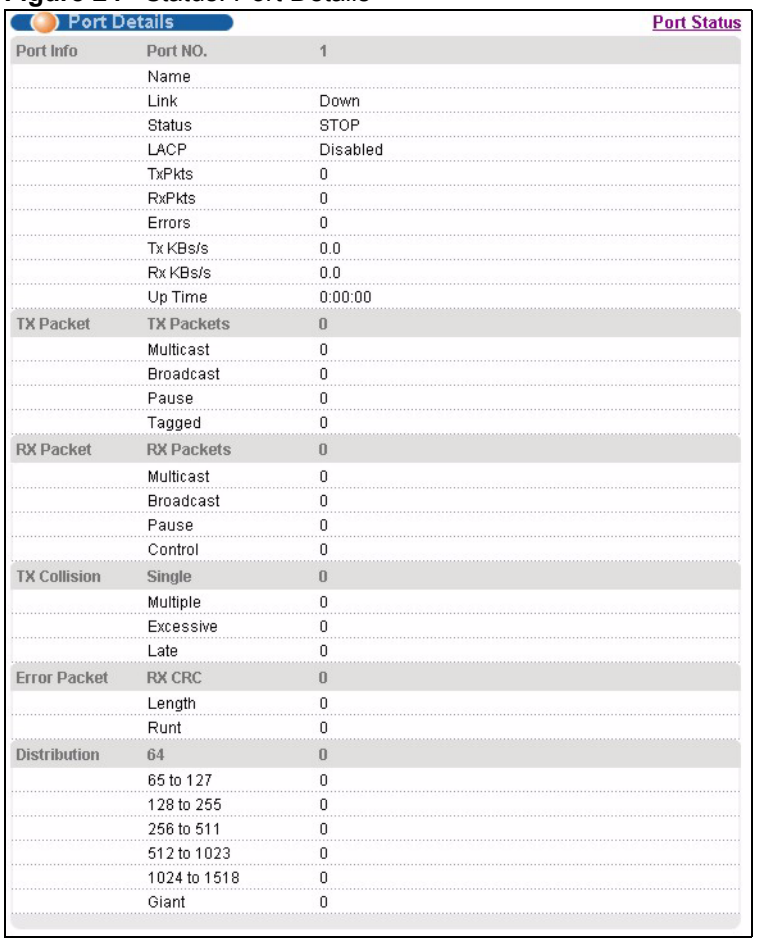
Table 7 Status

LABEL	DESCRIPTION
Port	This identifies the Ethernet port. Click a port number to display the **Port Details** screen (refer to Figure 24 on page 69).
Name	This is the name you assigned to this port in the **Basic Setting** > **Port Setup** screen.
Link	This field displays the speed (either **10M** for 10 Mbps, **100M** for 100 Mbps, **1000M** for 1000 Mbps, and **10G** for 10 Gbps) and the duplex (**F** for full duplex or **H** for half). It also shows the cable type (**Copper** or **Fiber**) for the combo ports.
State	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port. (see Section 11.1.3 on page 108 for more information). If STP is disabled, this field displays **FORWARDING** if the link is up, otherwise, it displays **STOP**.
LACP	This fields displays whether LACP (Link Aggregation Control Protocol) has been enabled on the port.
TxPkts	This field shows the number of transmitted frames on this port.
RxPkts	This field shows the number of received frames on this port.
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the transmission speed of data sent on this port in kilobytes per second.
Rx KB/s	This field shows the transmission speed of data received on this port in kilobytes per second.
Up Time	This field shows the total amount of time in hours, minutes and seconds the port has been up.
Clear Counter	Type a port number, select **Port** and then click **Clear Counter** to erase the recorded statistical information for that port, or select **Any** to clear statistics for all ports.

6.2.1 Status: Port Details

Click a number in the **Port** column in the **Status** screen to display individual port statistics. Use this screen to check status and detailed performance data about an individual port on the Switch.

Figure 24 Status: Port Details



Port Info	Port NO.	1
	Name	
	Link	Down
	Status	STOP
	LACP	Disabled
	TxPkts	0
	RxPkts	0
	Errors	0
	Tx KBs/s	0.0
	Rx KBs/s	0.0
	Up Time	0:00:00
TX Packet	TX Packets	0
	Multicast	0
	Broadcast	0
	Pause	0
	Tagged	0
RX Packet	RX Packets	0
	Multicast	0
	Broadcast	0
	Pause	0
	Control	0
TX Collision	Single	0
	Multiple	0
	Excessive	0
	Late	0
Error Packet	RX CRC	0
	Length	0
	Runt	0
Distribution	64	0
	65 to 127	0
	128 to 255	0
	256 to 511	0
	512 to 1023	0
	1024 to 1518	0
	Giant	0

The following table describes the labels in this screen.

Table 8 Status > Port Details

LABEL	DESCRIPTION
Port Info	
Port NO.	This field displays the port number you are viewing.
Name	This field displays the name of the port.
Link	This field displays the speed (either **10M** for 10Mbps, **100M** for 100Mbpsl, **1000M** for 1000 Mbps, and **10G** for 10 Gbps) and the duplex (**F** for full duplex or **H** for half duplex). It also shows the cable type (**Copper** or **Fiber**).
Status	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port (see Section 11.1.3 on page 108 for more information). If STP is disabled, this field displays FORWARDING if the link is up, otherwise, it displays STOP.
LACP	This field shows if LACP is enabled on this port or not.
TxPkts	This field shows the number of transmitted frames on this port
RxPkts	This field shows the number of received frames on this port
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the transmission speed of data sent on this port in kilobytes per second.

Table 8 Status > Port Details (continued)

LABEL	DESCRIPTION
Rx KB/s	This field shows the transmission speed of data received on this port in kilobytes per second.
Up Time	This field shows the total amount of time the connection has been up.
Tx Packet The following fields display detailed information about packets transmitted.	
TX Packets	This field shows the number of good packets (unicast, multicast and broadcast) transmitted.
Multicast	This field shows the number of good multicast packets transmitted.
Broadcast	This field shows the number of good broadcast packets transmitted.
Pause	This field shows the number of 802.3x Pause packets transmitted.
Tagged	This field shows the number of packets with VLAN tags transmitted.
Rx Packet The following fields display detailed information about packets received.	
RX Packets	This field shows the number of good packets (unicast, multicast and broadcast) received.
Multicast	This field shows the number of good multicast packets received.
Broadcast	This field shows the number of good broadcast packets received.
Pause	This field shows the number of 802.3x Pause packets received.
Control	This field shows the number of control packets received (including those with CRC error) but it does not include the 802.3x Pause packets.
TX Collision The following fields display information on collisions while transmitting.	
Single	This is a count of successfully transmitted packets for which transmission is inhibited by exactly one collision.
Multiple	This is a count of successfully transmitted packets for which transmission was inhibited by more than one collision.
Excessive	This is a count of packets for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Late	This is the number of times a late collision is detected, that is, after 512 bits of the packets have already been transmitted.
Error Packet	The following fields display detailed information about packets received that were in error.
RX CRC	This field shows the number of packets received with CRC (Cyclic Redundant Check) error(s).
Length	This field shows the number of packets received with a length that was out of range.
Runt	This field shows the number of packets received that were too short (shorter than 64 octets), including the ones with CRC errors.
Distribution	
64	This field shows the number of packets (including bad packets) received that were 64 octets in length.
65-127	This field shows the number of packets (including bad packets) received that were between 65 and 127 octets in length.
128-255	This field shows the number of packets (including bad packets) received that were between 128 and 255 octets in length.

Table 8 Status > Port Details (continued)

LABEL	DESCRIPTION
256-511	This field shows the number of packets (including bad packets) received that were between 256 and 511 octets in length.
512-1023	This field shows the number of packets (including bad packets) received that were between 512 and 1023 octets in length.
1024-1518	This field shows the number of packets (including bad packets) received that were between 1024 and 1518 octets in length.
Giant	This field shows the number of packets dropped because they were bigger than the maximum frame size.

7

Basic Setting

This chapter describes how to configure the **System Info, General Setup**, **Switch Setup**, **IP Setup** and **Port Setup** screens.

7.1 Overview

The **System Info** screen displays general Switch information (such as firmware version number) and hardware polling information (such as fan speeds). The **General Setup** screen allows you to configure general Switch identification information. The **General Setup** screen also allows you to set the system time manually or get the current time and date from an external server when you turn on your Switch. The real time is then displayed in the Switch logs. The **Switch Setup** screen allows you to set up and configure global Switch features. The **IP Setup** screen allows you to configure a Switch IP address in each routing domain, subnet mask(s) and DNS (domain name server) for management purposes.

7.2 System Information

In the navigation panel, click **Basic Setting** > **System Info** to display the screen as shown. You can check the firmware version number and monitor the Switch temperature, fan speeds and voltage in this screen.

Figure 25 Basic Setting > System Info

System Info
System Name
XGS-4528F
ZyNOS F/W Version
V3.80(ARC.0)b4 | 07/04/2007
Ethernet Address
00:13:49:01:1f:b0
Hardware Monitor
Temperature Unit C
Temperature (C) Current MAX MIN Threshold Status
BOARD -1.0 -1.0 -1.0 75.0 Normal
PHY -1.0 -1.0 -1.0 85.0 Normal
MAC -1.0 -1.0 -1.0 85.0 Normal
FAN Speed (RPM) Current MAX MIN Threshold Status
FAN1 < 41 0 0 3100 Normal
FAN2 < 41 0 0 3100 Normal
FAN3 < 41 0 0 3100 Normal
Voltage (V) Current MAX MIN Threshold Status
1.2VIN 0.-02 0.-02 0.-02 +/-8% Error
1.25VIN 0.-02 0.-02 0.-02 +/-8% Error
1.8VIN 0.-02 0.-02 0.-02 +/-9% Error
3.3VIN 0.-02 0.-02 0.-02 +/-8% Error
12VIN 0.-02 0.-02 0.-02 +/-10% Error

The following table describes the labels in this screen.

Table 9 Basic Setting > System Info

LABEL	DESCRIPTION
System Name	This field displays the descriptive name of the Switch for identification purposes.
ZyNOS F/W Version	This field displays the version number of the Switch 's current firmware including the date created.
Ethernet Address	This field refers to the Ethernet MAC (Media Access Control) address of the Switch.
Hardware Monitor	
Temperature Unit	The Switch has temperature sensors that are capable of detecting and reporting if the temperature rises above the threshold. You may choose the temperature unit (Centigrade or Fahrenheit) in this field.
Temperature	**BOARD, PHY**, and **MAC** refer to the location of the temperature sensors on the Switch printed circuit board.
Current	This shows the current temperature at this sensor.
MAX	This field displays the maximum temperature measured at this sensor.
MIN	This field displays the minimum temperature measured at this sensor.
Threshold	This field displays the upper temperature limit at this sensor.
Status	This field displays **Normal** for temperatures below the threshold and **Error** for those above.
Fan Speed (RPM)	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that is capable of detecting and reporting if the fan speed falls below the threshold shown.
Current	This field displays this fan's current speed in Revolutions Per Minute (RPM).
MAX	This field displays this fan's maximum speed measured in RPM.
MIN	This field displays this fan's minimum speed measured in RPM. “<41" is displayed for speeds too small to measure (under 2000 RPM).

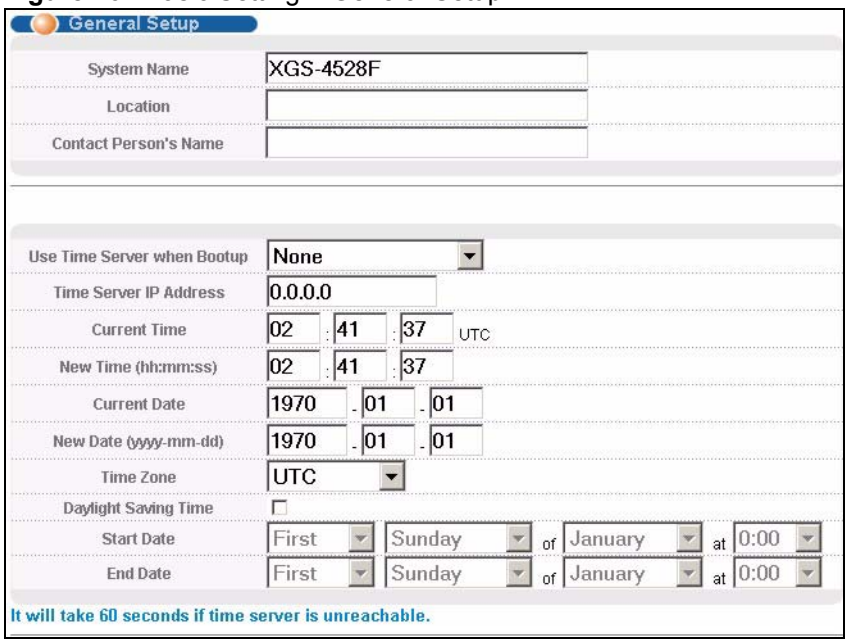
Table 9 Basic Setting > System Info (continued)

LABEL	DESCRIPTION
Threshold	This field displays the minimum speed at which a normal fan should work.
Status	**Normal** indicates that this fan is functioning above the minimum speed. **Error** indicates that this fan is functioning below the minimum speed.
Voltage (V)	The power supply for each voltage has a sensor that is capable of detecting and reporting if the voltage falls out of the tolerance range.
Current	This is the current voltage reading.
MAX	This field displays the maximum voltage measured at this point.
MIN	This field displays the minimum voltage measured at this point.
Threshold	This field displays the percentage tolerance of the voltage with which the Switch still works.
Status	**Normal** indicates that the voltage is within an acceptable operating range at this point; otherwise **Error** is displayed.

7.3 General Setup

Use this screen to configure general settings such as the system name and time. Click **Basic Setting** and **General Setup** in the navigation panel to display the screen as shown.

Figure 26 Basic Setting > General Setup



The following table describes the labels in this screen.

Table 10 Basic Setting > General Setup

LABEL	DESCRIPTION
System Name	Type a descriptive name for identification purposes. This name consists of up to 64 printable characters; spaces are allowed.
Location	Type the geographic location of your Switch. You can use up to 32 printable ASCII characters; spaces are allowed.

Table 10 Basic Setting > General Setup (continued)

LABEL	DESCRIPTION
Contact Person's Name	Type the name of the person in charge of this Switch. You can use up to 32 printable ASCII characters; spaces are allowed.
Use Time Server when Bootup	Type the time service protocol that your timeserver uses. Not all time servers support all protocols, so you may have to use trial and error to find a protocol that works. The main differences between them are the time format. When you select the **Daytime (RFC 867)** format, the Switch displays the day, month, year and time with no time zone adjustment. When you use this format, it is recommended that you use a Daytime timeserver within your geographical time zone. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC-1305)** is similar to Time (RFC-868). **None** is the default value. Enter the time manually. Each time you turn on the Switch, the time and date will be reset to 1970-1-1 0:0.
Time Server IP Address	Type the IP address of your timeserver. The Switch searches for the timeserver for up to 60 seconds. If you select a timeserver that is unreachable, then this screen will appear locked for 60 seconds. Please wait.
Current Time	This field displays the time you open this menu (or refresh the menu).
New Time (hh:min:ss)	Enter the new time in hour, minute and second format. The new time then appears in the **Current Time** field after you click **Apply**.
Current Date	This field displays the date you open this menu.
New Date (yyyy-mm-dd)	Enter the new date in year, month and day format. The new date then appears in the **Current Date** field after you click **Apply**.
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box.
Daylight Saving Time	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Saving Time**. The time is displayed in the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and **2:00**. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March** and the last field depends on your time zone. In Germany for instance, you would select **2:00** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

Table 10 Basic Setting > General Setup (continued)

LABEL	DESCRIPTION
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Saving Time**. The time field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and **2:00**. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October** and the last field depends on your time zone. In Germany for instance, you would select **2:00** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

7.4 Introduction to VLANs

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In MTU (Multi-Tenant Unit) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user on the same network.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

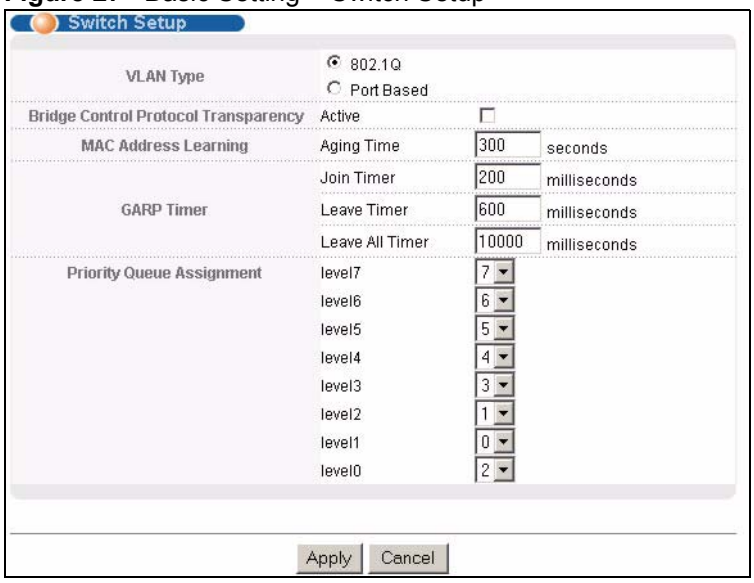
VLAN is unidirectional; it only governs outgoing traffic.

See Chapter 8 on page 87 for information on port-based and 802.1Q tagged VLANs.

7.5 Switch Setup Screen

Click **Basic Setting** and then **Switch Setup** in the navigation panel to display the screen as shown. The VLAN setup screens change depending on whether you choose **802.1Q** or **Port Based** in the **VLAN Type** field in this screen. Refer to the chapter on VLAN.

Figure 27 Basic Setting > Switch Setup



The following table describes the labels in this screen.

Table 11 Basic Setting > Switch Setup

LABEL	DESCRIPTION
VLAN Type	Choose **802.1Q** or **Port Based**. The **VLAN Setup** screen changes depending on whether you choose **802.1Q** VLAN type or **Port Based** VLAN type in this screen. See Chapter 8 on page 87 for more information.
Bridge Control Protocol Transparency	Select **Active** to allow the Switch to handle bridging control protocols (STP, for example). You also need to define how to treat a BPDU in the **Port Setup** screen.
MAC Address Learning	MAC address learning reduces outgoing traffic broadcasts. For MAC address learning to occur on a port, the port must be active.
Aging Time	Enter a time from 10 to 3000 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned).
GARP Timer: Switches join VLANs by making a declaration. A declaration is made by issuing a **Join** message using GARP. Declarations are withdrawn by issuing a **Leave** message. A **Leave All** message terminates all registrations. GARP timers set declaration timeout values. See Chapter 8 on page 87 for more background information.	
Join Timer	Join Timer sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a **Join Period** timer. The allowed **Join Time** range is between 100 and 65535 milliseconds; the default is 200 milliseconds. See Chapter 8 on page 87 for more background information.
Leave Timer	Leave Time sets the duration of the **Leave Period** timer for GVRP in milliseconds. Each port has a single **Leave Period** timer. Leave Time must be two times larger than **Join Timer**; the default is 600 milliseconds.
Leave All Timer	Leave All Timer sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer.

Table 11 Basic Setting > Switch Setup (continued)

LABEL	DESCRIPTION
Priority Queue Assignment IEEE 802.1p defines up to eight separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. Use the following fields to configure the priority level-to-physical queue mapping. The Switch has eight physical queues that you can map to the 8 priority levels. On the Switch, traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested.	
Priority Level (The following descriptions are based on the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).	
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for “spare bandwidth”.
Level 1	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.
Apply	Click **Apply** to save your changes to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

7.6 IP Setup

Use the **IP Setup** screen to configure the default gateway device, the default domain name server and add IP domains.

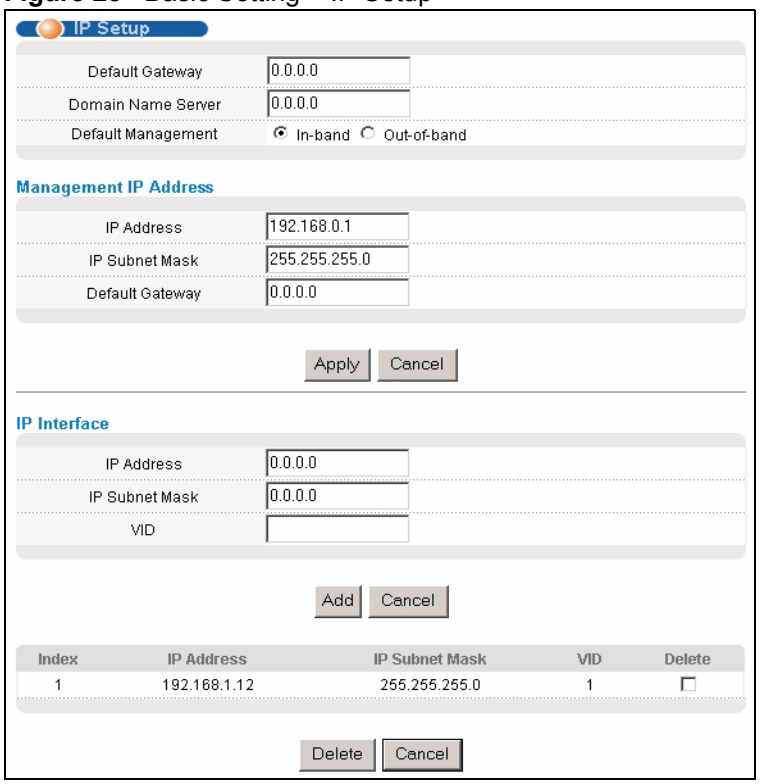
7.6.1 IP Interfaces

The Switch needs an IP address for it to be managed over the network. The factory default IP address is 192.168.1.1. The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0.

On the Switch, as a layer-3 device, an IP address is not bound to any physical ports. Since each IP address on the Switch must be in a separate subnet, the configured IP address is also known as IP interface (or routing domain). In addition, this allows routing between subnets based on the IP address without additional routers.

You can configure multiple routing domains on the same VLAN as long as the IP address ranges for the domains do not overlap. To change the IP address of the Switch in a routing domain, simply add a new routing domain entry with a different IP address in the same subnet.

Figure 28 Basic Setting > IP Setup



The following table describes the labels in this screen.

Table 12 Basic Setting > IP Setup

LABEL	DESCRIPTION
Default Gateway	Type the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
Domain Name Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. Enter a domain name server IP address in order to be able to use a domain name instead of an IP address.
Default Management	Specify which traffic flow (**In-Band** or **Out-of-band**) the Switch is to send packets originating from itself (such as SNMP traps) or packets with unknown source. Select **Out-of-band** to have the Switch send the packets to the management port labelled **MGMT**. This means that device(s) connected to the other port(s) do not receive these packets. Select **In-Band** to have the Switch send the packets to all ports except the management port (labelled **MGMT**) to which connected device(s) do not receive these packets.
Management IP Address Use these fields to set the settings for the out-of-band management port.	
IP Address	Enter the out-of-band management IP address of your Switch in dotted decimal notation. For example, 192.168.0.1.
IP Subnet Mask	Enter the IP subnet mask of your Switch in dotted decimal notation, for example, 255.255.255.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example, 192.168.0.254

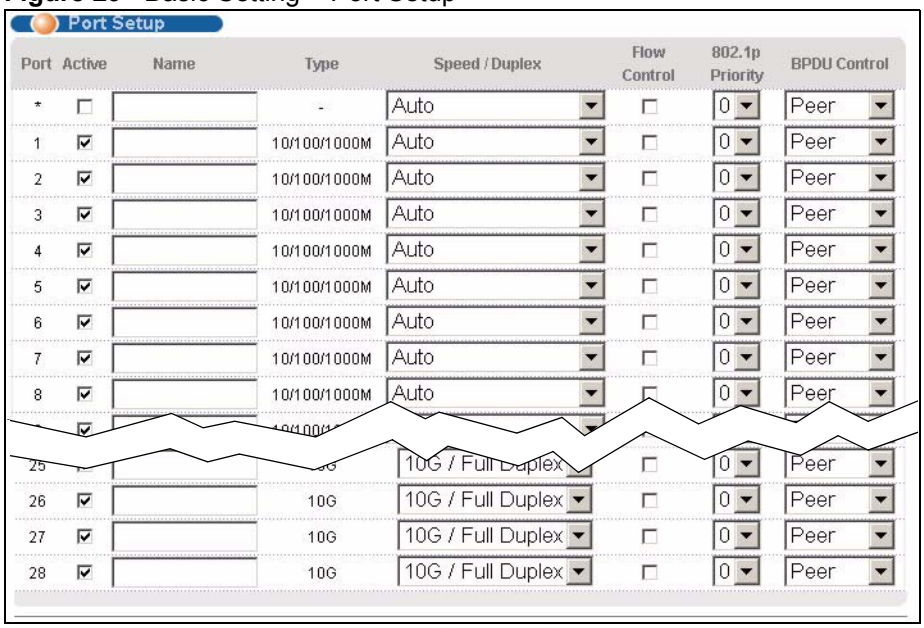
Table 12 Basic Setting > IP Setup (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
IP Interface Use these fields to create or edit IP routing domains on the Switch.	
IP Address	Enter the IP address of your Switch in dotted decimal notation, for example, 192.168.1.1. This is the IP address of the Switch in an IP routing domain.
IP Subnet Mask	Enter the IP subnet mask of an IP routing domain in dotted decimal notation, for example, 255.255.255.0.
VID	Enter the VLAN identification number to which an IP routing domain belongs.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Index	This field displays the index number of an entry.
IP Address	This field displays IP address of the Switch in the IP domain.
IP Subnet Mask	This field displays the subnet mask of the Switch in the IP domain.
VID	This field displays the VLAN identification number of the IP domain on the Switch.
Delete	Click **Delete** to remove the selected entry from the summary table. Note: Deleting all IP subnets locks you out of the Switch.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

7.7 Port Setup

Use this screen to configure Switch port settings.Click **Basic Setting** > **Port Setup** in the navigation panel to display the configuration screen.

Figure 29 Basic Setting > Port Setup



The following table describes the labels in this screen.

Table 13 Basic Setting > Port Setup

LABEL	DESCRIPTION
Port	This is the port index number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable a port. The factory default for all ports is enabled. A port must be enabled for data transmission to occur.
Name	Type a descriptive name that identifies this port. You can enter up to 64 alpha-numerical characters. Note: Due to space limitations, the port name may be truncated in some web configurator screens.
Type	This field displays **10/100/1000M** for a 1000Base-T connection and **10G** for a 10 Gigabit Ethernet connection.

Table 13 Basic Setting > Port Setup (continued)

LABEL	DESCRIPTION
Speed/Duplex	Select the speed and the duplex mode of the Ethernet connection on this port. The choices are **Auto**, **10M/Half Duplex**, **10M/Full Duplex**, **100M/Half Duplex** and **100M/Full Duplex** for a 1000Base-T connection. **1000M/Full Duplex** is supported by both 1000Base-T and 1000Base-X connections. **10G/Full Duplex** is supported by the 10 Gigabit Ethernet connections. Selecting **Auto** (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the Switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the Switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.
Flow Control	A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. **Flow Control** is used to regulate transmission of signals to match the bandwidth of the receiving port. The Switch uses IEEE 802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE 802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. Select **Flow Control** to enable it.
802.1p Priority	This priority value is added to incoming frames without a (802.1p) priority queue tag. See **Priority Queue Assignment** in Table 11 on page 78 for more information.
BPDU Control	Configure the way to treat BPDUs received on this port. You must activate bridging control protocol transparency in the **Switch Setup** screen first. Select **Peer** to process any BPDU (Bridge Protocol Data Units) received on this port. Select **Tunnel** to forward BPDUs received on this port. Select **Discard** to drop any BPDU received on this port. Select **Network** to process a BPDU with no VLAN tag and forward a tagged BPDU.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

PART III
Advanced Setup

VLAN (87)
Static MAC Forward Setup (103)
Filtering (105)
Spanning Tree Protocol (107)
Bandwidth Control (127)
Broadcast Storm Control (129)
Mirroring (131)
Link Aggregation (133)
Port Authentication (141)
Port Security (147)
Classifier (151)
Policy Rule (157)
Queuing Method (163)
VLAN Stacking (167)
Multicast (173)
Authentication & Accounting (187)
IP Source Guard (201)
Loop Guard (221)

8

VLAN

The type of screen you see here depends on the **VLAN Type** you selected in the **Switch Setup** screen. This chapter shows you how to configure 802.1Q tagged and port-based VLANs.

8.1 Introduction to IEEE 802.1Q Tagged VLANs

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes for the TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes for the TCI (Tag Control Information, starting after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and the value 4095 (FFF) is reserved, so the maximum possible number of VLAN configurations is 4,094.

TPID 2 Bytes	User Priority 3 Bits	CFI 1 Bit	VLAN ID 12 bits

8.1.1 Forwarding Tagged and Untagged Frames

Each port on the Switch is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the Switch first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the Switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

A broadcast frame (or a multicast frame for a multicast group that is known by the system) is duplicated only on ports that are members of the VID (except the ingress port itself), thus confining the broadcast to a specific domain.

8.2 Automatic VLAN Registration

GARP and GVRP are the protocols used to automatically register VLAN membership across switches.

8.2.1 GARP

GARP (Generic Attribute Registration Protocol) allows network switches to register and de-register attribute values with other GARP participants within a bridged LAN. GARP is a protocol that provides a generic mechanism for protocols that serve a more specific application, for example, GVRP.

8.2.1.1 GARP Timers

Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values.

8.2.2 GVRP

GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Enable this function to permit VLAN groups beyond the local Switch.

Please refer to the following table for common IEEE 802.1Q VLAN terminology.

Table 14 IEEE 802.1Q VLAN Terminology

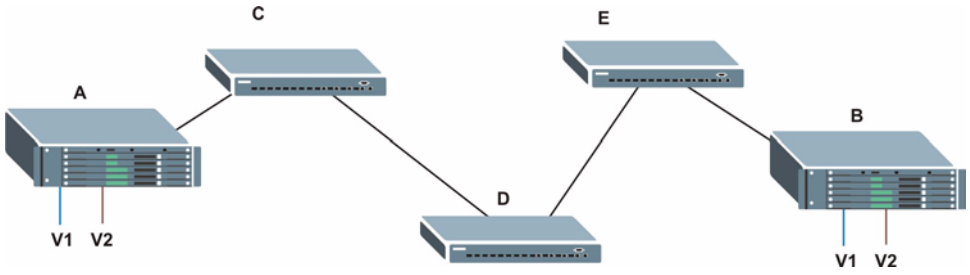
VLAN PARAMETER	TERM	DESCRIPTION
VLAN Type	Permanent VLAN	This is a static VLAN created manually.
	Dynamic VLAN	This is a VLAN configured by a GVRP registration/ deregistration process.
VLAN Administrative Control	Registration Fixed	Fixed registration ports are permanent VLAN members.
	Registration Forbidden	Ports with registration forbidden are forbidden to join the specified VLAN.
	Normal Registration	Ports dynamically join a VLAN using GVRP.
VLAN Tag Control	Tagged	Ports belonging to the specified VLAN tag all outgoing frames transmitted.
	Untagged	Ports belonging to the specified VLAN don't tag all outgoing frames transmitted.
VLAN Port	Port VID	This is the VLAN ID assigned to untagged frames that this port received.
	Acceptable Frame Type	You may choose to accept both tagged and untagged incoming frames, just tagged incoming frames or just untagged incoming frames on a port.
	Ingress filtering	If set, the Switch discards incoming frames for VLANs that do not have this port as a member.

8.3 Port VLAN Trunking

Enable **VLAN Trunking** on a port to allow frames belonging to unknown VLAN groups to pass through that port. This is useful if you want to set up VLAN groups on end devices without having to configure the same VLAN groups on intermediary devices.

The following figure describes **VLAN Trunking**. Suppose you want to create VLAN groups 1 and 2 (V1 and V2) on devices A and B. Without **VLAN Trunking,** you must configure VLAN groups 1 and 2 on all intermediary switches C, D and E; otherwise they will drop frames with unknown VLAN group tags. However, with **VLAN Trunking** enabled on a port(s) in each intermediary switch you only need to create VLAN groups in the end devices (A and B). C, D and E automatically allow frames with VLAN group tags 1 and 2 (VLAN groups that are unknown to those switches) to pass through their VLAN trunking port(s).

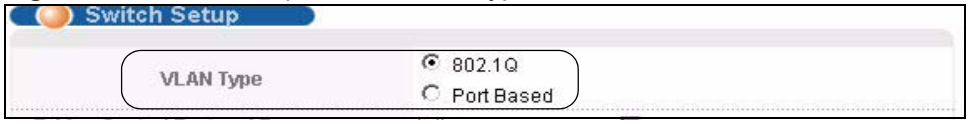
Figure 30 Port VLAN Trunking



8.4 Select the VLAN Type

Select a VLAN type in the **Basic Setting > Switch Setup** screen.

Figure 31 Switch Setup: Select VLAN Type



8.5 Static VLAN

Use a static VLAN to decide whether an incoming frame on a port should be

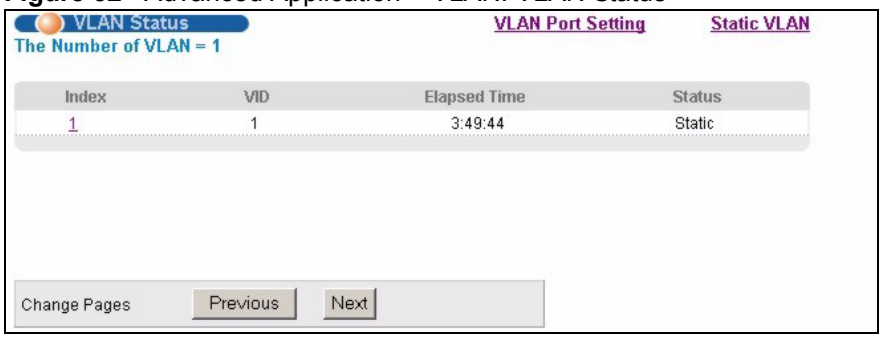
- sent to a VLAN group as normal depending on its VLAN tag.
- sent to a group whether it has a VLAN tag or not.
- blocked from a VLAN group regardless of its VLAN tag.

You can also tag all outgoing frames (that were previously untagged) from a port with the specified VID.

8.5.1 Static VLAN Status

See Section 8.1 on page 87 for more information on Static VLAN. Click **Advanced Application** > **VLAN** from the navigation panel to display the **VLAN Status** screen as shown next.

Figure 32 Advanced Application > VLAN: VLAN Status



The following table describes the labels in this screen.

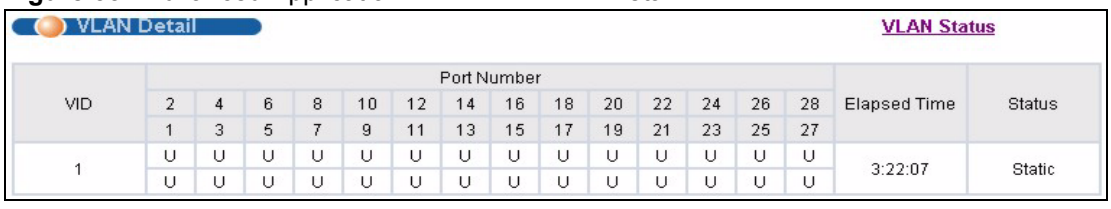
Table 15 Advanced Application > VLAN: VLAN Status

LABEL	DESCRIPTION
The Number of VLAN	This is the number of VLANs configured on the Switch.
Index	This is the VLAN index number. Click on an index number to view more VLAN details.
VID	This is the VLAN identification number that was configured in the **Static VLAN** screen.
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the Switch; **dynamic** - using GVRP, **static** - added as a permanent entry or **other** - added in another way such as via Multicast VLAN Registration (MVR).
Change Pages	Click **Previous** or **Next** to show the previous/next screen if all status information cannot be seen in one screen.

8.5.2 Static VLAN Details

Use this screen to view detailed port settings and status of the VLAN group. See Section 8.1 on page 87 for more information on static VLAN. Click on an index number in the **VLAN Status** screen to display VLAN details.

Figure 33 Advanced Application > VLAN > VLAN Detail


VLAN Detail
VLAN Status
VID
Port Number
2 4 6 8 10 12 14 16 18 20 22 24 26 28
1 3 5 7 9 11 13 15 17 19 21 23 25 27
Elapsed Time
Status
1
U U U U U U U U U U U U U U
U U U U U U U U U U U U U U
3:22:07
Static

The following table describes the labels in this screen.

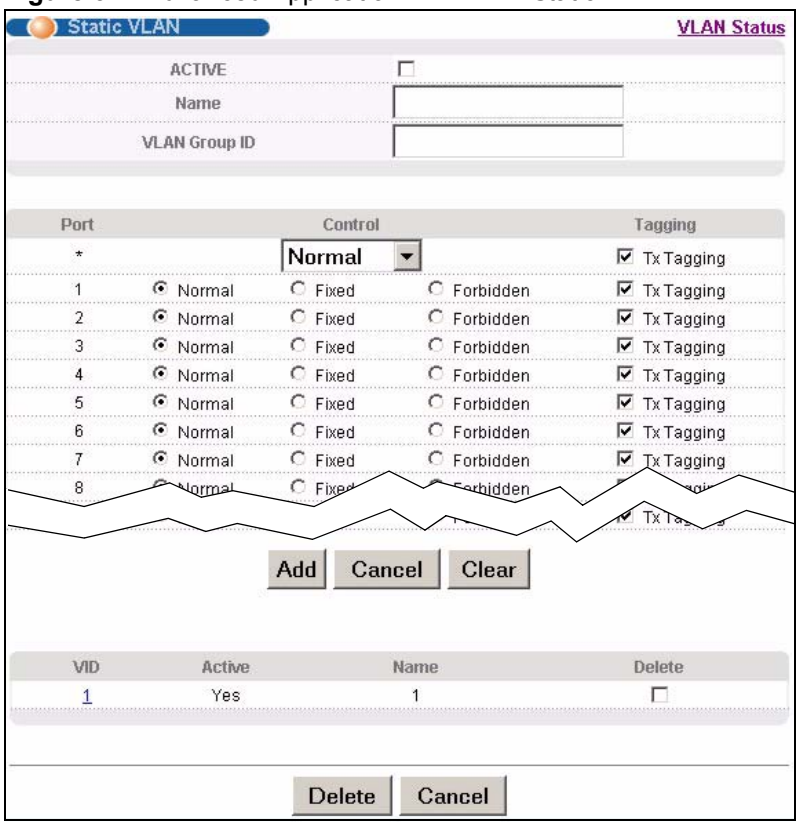
Table 16 Advanced Application > VLAN > VLAN Detail

LABEL	DESCRIPTION
VLAN Status	Click this to go to the **VLAN Status** screen.
VID	This is the VLAN identification number that was configured in the **Static VLAN** screen.
Port Number	This column displays the ports that are participating in a VLAN. A tagged port is marked as **T**, an untagged port is marked as **U** and ports not participating in a VLAN are marked as "**–**".
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the Switch; **dynamic** - using GVRP, **static** - added as a permanent entry or **other** - added in another way such as via Multicast VLAN Registration (MVR).

8.5.3 Configure a Static VLAN

Use this screen to configure and view 802.1Q VLAN parameters for the Switch. See Section 8.1 on page 87 for more information on static VLAN. To configure a static VLAN, click **Static VLAN** in the **VLAN Status** screen to display the screen as shown next.

Figure 34 Advanced Application > VLAN > Static VLAN



The following table describes the related labels in this screen.

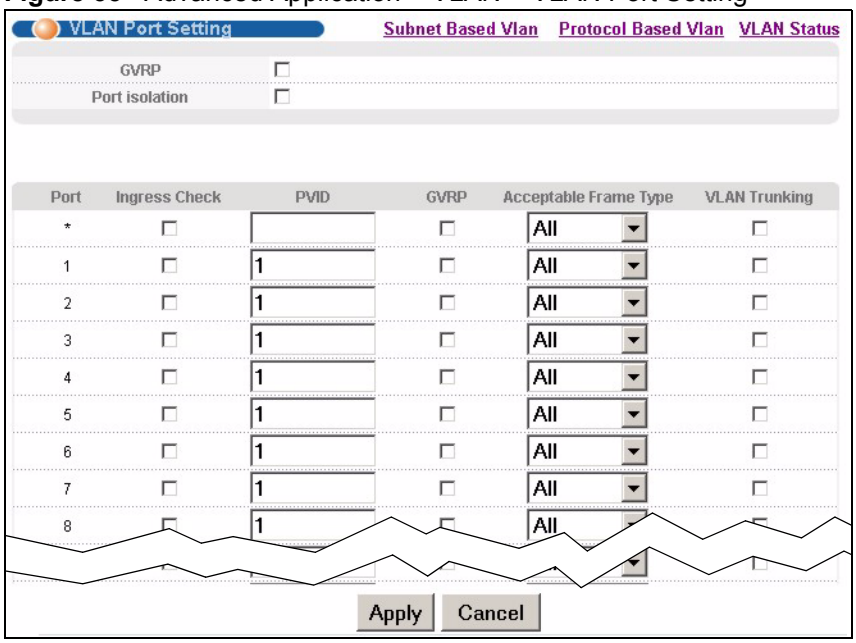
Table 17 Advanced Application > VLAN > Static VLAN

LABEL	DESCRIPTION
ACTIVE	Select this check box to activate the VLAN settings.
Name	Enter a descriptive name for the VLAN group for identification purposes. This name consists of up to 64 printable characters; spaces are allowed.
VLAN Group ID	Enter the VLAN ID for this static entry; the valid range is between 1 and 4094.
Port	The port number identifies the port you are configuring.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Control	Select **Normal** for the port to dynamically join this VLAN group using GVRP. This is the default selection. Select **Fixed** for the port to be a permanent member of this VLAN group. Select **Forbidden** if you want to prohibit the port from joining this VLAN group.
Tagging	Select **TX Tagging** if you want the port to tag all outgoing frames transmitted with this VLAN Group ID.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to start configuring the screen again.
VID	This field displays the ID number of the VLAN group. Click the number to edit the VLAN settings.
Active	This field indicates whether the VLAN settings are enabled (**Yes**) or disabled (**No**).
Name	This field displays the descriptive name for this VLAN group.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

8.5.4 Configure VLAN Port Settings

Use the VLAN Port Setting screen to configure the static VLAN (IEEE 802.1Q) settings on a port. See Section 8.1 on page 87 for more information on static VLAN. Click the **VLAN Port Setting** link in the **VLAN Status** screen.

Figure 35 Advanced Application > VLAN > VLAN Port Setting



The following table describes the labels in this screen.

Table 18 Advanced Application > VLAN > VLAN Port Setting

LABEL	DESCRIPTION
GVRP	GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Select this check box to permit VLAN groups beyond the local Switch.
Port Isolation	**Port Isolation** allows each port to communicate only with the CPU management port and the uplink ports but not communicate with each other. This option is the most limiting but also the most secure.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Ingress Check	If this check box is selected for a port, the Switch discards incoming frames for VLANs that do not include this port in its member set. Clear this check box to disable ingress filtering.
PVID	Enter a number between 1and 4094 as the port VLAN ID.
GVRP	Select this check box to allow GVRP on this port.
Acceptable Frame Type	Specify the type of frames allowed on a port. Choices are **All** and **Tag Only**. Select **All** from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting. Select **Tag Only** to accept only tagged frames on this port. All untagged frames will be dropped.

Table 18 Advanced Application > VLAN > VLAN Port Setting (continued)

LABEL	DESCRIPTION
VLAN Trunking	Enable **VLAN Trunking** on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the Switch.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

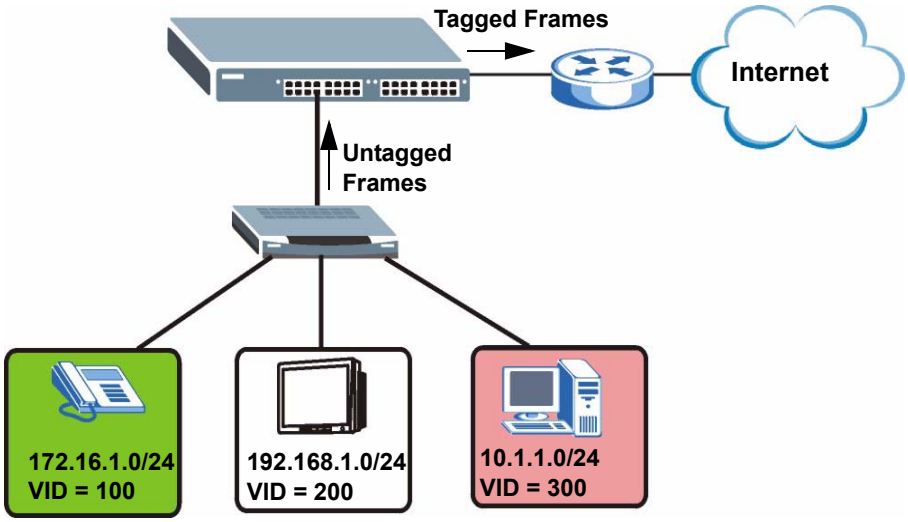
8.6 Subnet Based VLANs

Subnet based VLANs allow you to group traffic into logical VLANs based on the source IP subnet you specify. When a frame is received on a port, the Switch checks if a tag is added already and the IP subnet it came from. The untagged packets from the same IP subnet are then placed in the same subnet based VLAN. One advantage of using subnet based VLANs is that priority can be assigned to traffic from the same IP subnet.

For example, an ISP (Internet Service Provider) may divide different types of services it provides to customers into different IP subnets. Traffic for voice services is designated for IP subnet 172.16.1.0/24, video for 192.168.1.0/24 and data for 10.1.1.0/24. The Switch can then be configured to group incoming traffic based on the source IP subnet of incoming frames.

You can then configure a subnet based VLAN with priority 6 and VID of 100 for traffic received from IP subnet 172.16.1.0/24 (voice services). You can also have a subnet based VLAN with priority 5 and VID of 200 for traffic received from IP subnet 192.168.1.0/24 (video services). Lastly, you can configure VLAN with priority 3 and VID of 300 for traffic received from IP subnet 10.1.1.0/24 (data services). All untagged incoming frames will be classified based on their source IP subnet and prioritized accordingly. That is, video services receive the highest priority and data the lowest.

Figure 36 Subnet Based VLAN Application Example

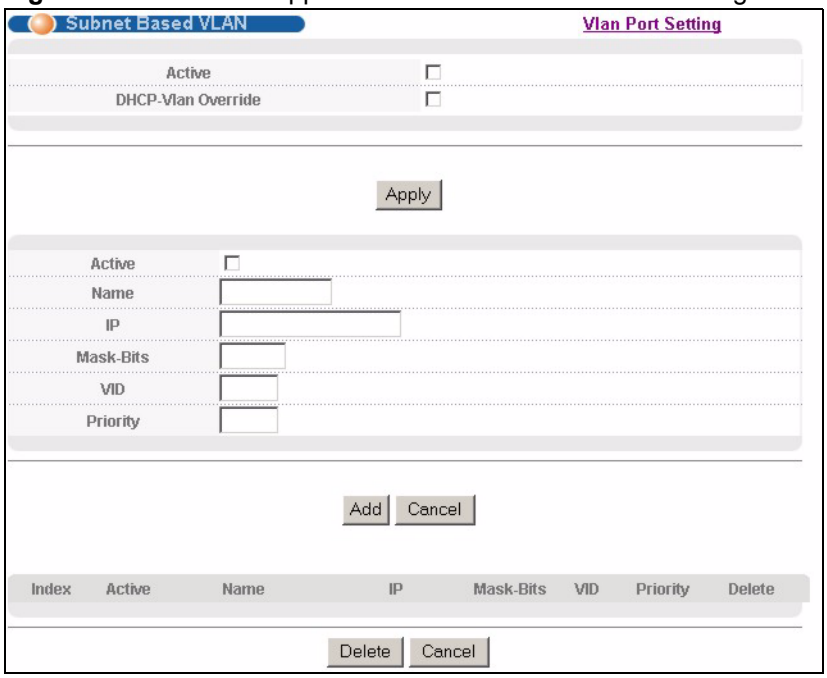


8.7 Configuring Subnet Based VLAN

Click **Subnet Based VLAN** in the **VLAN Port Setting** screen to display the configuration screen as shown.

Subnet based VLAN applies to un-tagged packets and is applicable only when you use IEEE 802.1Q tagged VLAN.

Figure 37 Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN



The following table describes the labels in this screen.

Table 19 Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN Setup

LABEL	DESCRIPTION
Active	Check this box to activate this subnet based VLANs on the Switch.
DHCP-Vlan Override	When DHCP snooping is enabled DHCP clients can renew their IP address through the DHCP VLAN or via another DHCP server on the subnet based VLAN. Select this checkbox to force the DHCP clients in this IP subnet to obtain their IP addresses through the DHCP VLAN.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Active	Check this box to activate the IP subnet VLAN you are creating or editing.
Name	Enter up to 32 alphanumeric characters to identify this subnet based VLAN.
IP	Enter the IP address of the subnet for which you want to configure this subnet based VLAN.

Table 19 Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN Setup

LABEL	DESCRIPTION
Mask-Bits	Enter the bit number of the subnet mask. To find the bit number, convert the subnet mask to binary format and add all the 1's together. Take "255.255.255.0" for example. 255 converts to eight 1s in binary. There are three 255s, so add three eights together and you get the bit number (24).
VID	Enter the ID of a VLAN with which the untagged frames from the IP subnet specified in this subnet based VLAN are tagged. This must be an existing VLAN which you defined in the **Advanced Applications > VLAN** screens.
Priority	Select the priority level that the Switch assigns to frames belonging to this VLAN.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Index	This is the index number identifying this subnet based VLAN. Click on any of these numbers to edit an existing subnet based VLAN.
Active	This field shows whether the subnet based VLAN is active or not.
Name	This field shows the name the subnet based VLAN.
IP	This field shows the IP address of the subnet for this subnet based VLAN.
Mask-Bits	This field shows the subnet mask in bit number format for this subnet based VLAN.
VID	This field shows the VLAN ID of the frames which belong to this subnet based VLAN.
Priority	This field shows the priority which is assigned to frames belonging to this subnet based VLAN.
Delete	Click this to delete the subnet based VLANs which you marked for deletion.
Cancel	Click **Cancel** to begin configuring this screen afresh.

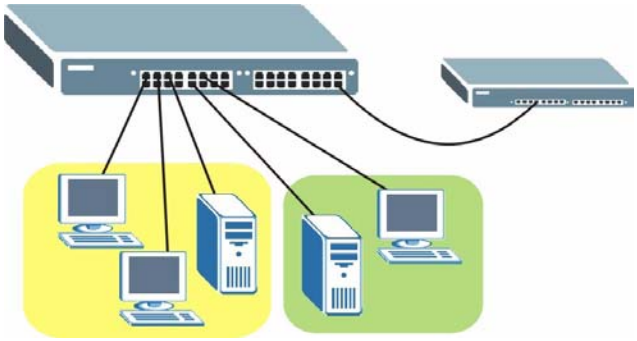
8.8 Protocol Based VLANs

Protocol based VLANs allow you to group traffic into logical VLANs based on the protocol you specify. When an upstream frame is received on a port (configured for a protocol based VLAN), the Switch checks if a tag is added already and its protocol. The untagged packets of the same protocol are then placed in the same protocol based VLAN. One advantage of using protocol based VLANs is that priority can be assigned to traffic of the same protocol.

Protocol based VLAN applies to un-tagged packets and is applicable only when you use IEEE 802.1Q tagged VLAN.

For example, ports 1, 2, 3 and 4 belong to static VLAN 100, and ports 4, 5, 6, 7 belong to static VLAN 120. You can configure a protocol based VLAN A with priority 3 for ARP traffic received on port 1, 2 and 3. You can also have a protocol based VLAN B with priority 2 for Apple Talk traffic received on port 6 and 7. All upstream ARP traffic from port 1, 2 and 3 will be grouped together, and all upstream Apple Talk traffic from port 6 and 7 will be in another group and have higher priority than ARP traffic when they go through the uplink port to a backbone switch C.

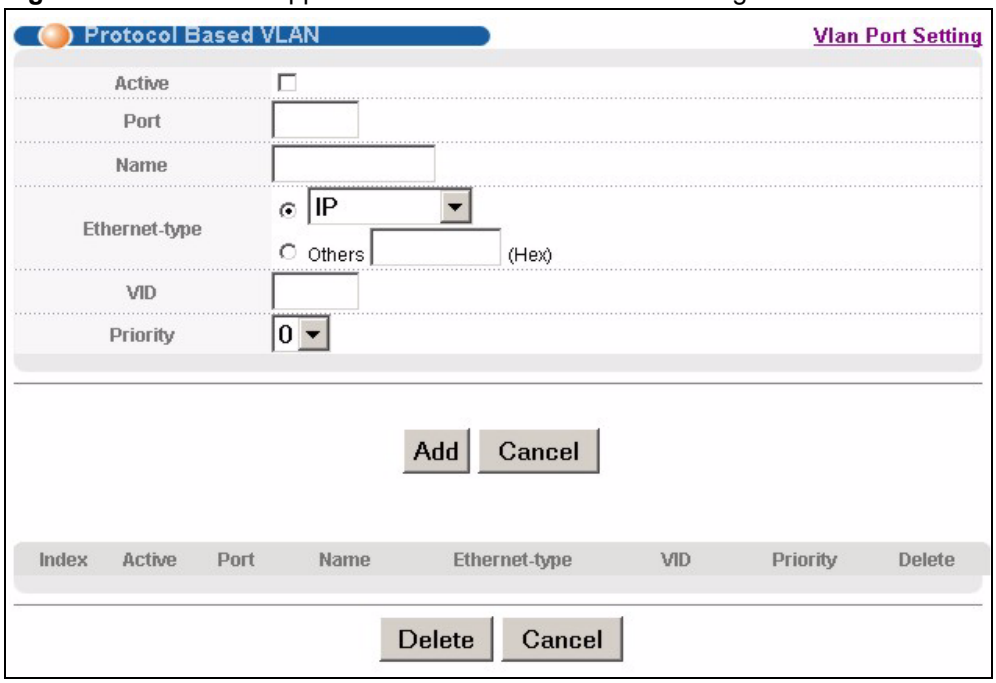
Figure 38 Protocol Based VLAN Application Example



8.9 Configuring Protocol Based VLAN

Click **Protocol Based VLAN** in the **VLAN Port Setting** screen to display the configuration screen as shown.

Figure 39 Advanced Application > VLAN > VLAN Port Setting > Protocol Based VLAN



The following table describes the labels in this screen.

Table 20 Advanced Application > VLAN > VLAN Port Setting > Protocol Based VLAN Setup

LABEL	DESCRIPTION
Active	Check this box to activate this protocol based VLAN.
Port	Type a port number to be included in this protocol based VLAN. This port must belong to a static VLAN in order to participate in a protocol based VLAN. See Chapter 8 on page 87 for more details on setting up VLANs.
Name	Enter up to 32 alphanumeric characters to identify this protocol based VLAN.
Ethernet-type	Use the drop down list box to select a predefined protocol to be included in this protocol based VLAN or select **Others** and type the protocol number in hexadecimal notation. For example, the IP protocol in hexadecimal notation is 0800, and Novell IPX protocol is 8137. Note: Protocols in the hexadecimal number range of 0x0000 to 0x05ff are not allowed to be used for protocol based VLANs.
VID	Enter the ID of a VLAN to which the port belongs. This must be an existing VLAN which you defined in the **Advanced Applications > VLAN** screens.
Priority	Select the priority level that the Switch will assign to frames belonging to this VLAN.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Index	This is the index number identifying this protocol based VLAN. Click on any of these numbers to edit an existing protocol based VLAN.
Active	This field shows whether the protocol based VLAN is active or not.
Port	This field shows which port belongs to this protocol based VLAN.
Name	This field shows the name the protocol based VLAN.
Ethernet-type	This field shows which Ethernet protocol is part of this protocol based VLAN.
VID	This field shows the VLAN ID of the port.
Priority	This field shows the priority which is assigned to frames belonging to this protocol based VLAN.
Delete	Click this to delete the protocol based VLANs which you marked for deletion.
Cancel	Click **Cancel** to begin configuring this screen afresh.

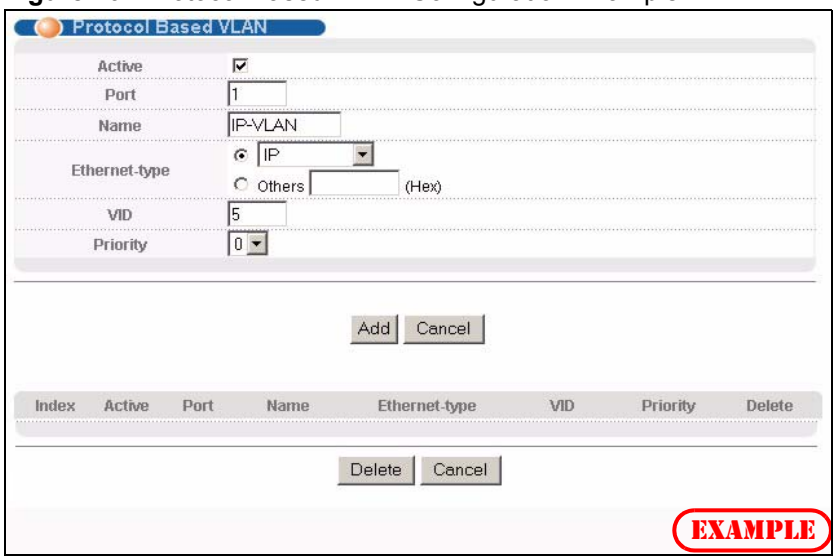
8.10 Create an IP-based VLAN Example

This example shows you how to create an IP VLAN which includes ports 1, 4 and 8. Follow these steps using the screen below:

1. Activate this protocol based VLAN.
2. Type the port number you want to include in this protocol based VLAN. Type **1**.
3. Give this protocol-based VLAN a descriptive name. Type **IP-VLAN**.
4. Select the protocol. Leave the default value **IP**.
5. Type the VLAN ID of an existing VLAN. In our example we already created a static VLAN with an ID of 5. Type **5**.

6 Leave the priority set to **0** and click **Add**.

Figure 40 Protocol Based VLAN Configuration Example



To add more ports to this protocol based VLAN.

1 Click the index number of the protocol based VLAN entry. Click **1**
2 Change the value in the **Port** field to the next port you want to add.
3 Click **Add**.

8.11 Port-based VLAN Setup

Port-based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

Port-based VLANs require allowed outgoing ports to be defined for each port. Therefore, if you wish to allow two subscriber ports to talk to each other, for example, between conference rooms in a hotel, you must define the egress (an egress port is an outgoing port, that is, a port through which a data packet leaves) for both ports.

Port-based VLANs are specific only to the Switch on which they were created.

When you activate port-based VLAN, the Switch uses a default VLAN ID of 1. You cannot change it.

In screens (such as **IP Setup** and **Filtering**) that require a VID, you must enter 1 as the VID.

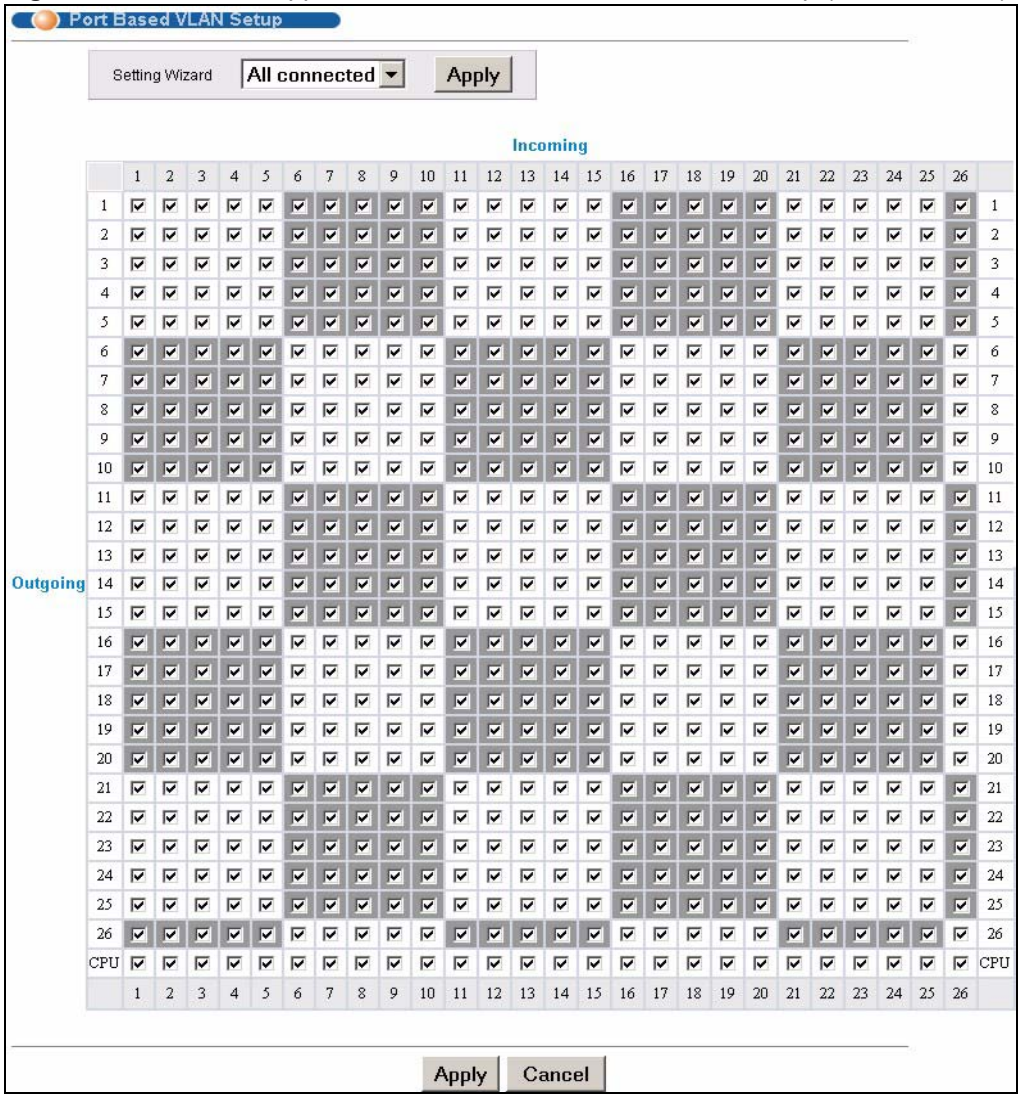
The port-based VLAN setup screen is shown next. The **CPU** management port forms a VLAN with all Ethernet ports.

8.11.1 Configure a Port-based VLAN

Select **Port Based** as the **VLAN Type** in the **Switch Setup** screen and then click **VLAN** from the navigation panel to display the following screen. Select either **All Connected** or **Port Isolated** from the drop-down list depending on your VLAN and VLAN security requirements. If VLAN members need to communicate directly with each other, then select **All Connected**. Select **Port Isolated** if you want to restrict users from communicating directly. Click **Apply** to save your settings.

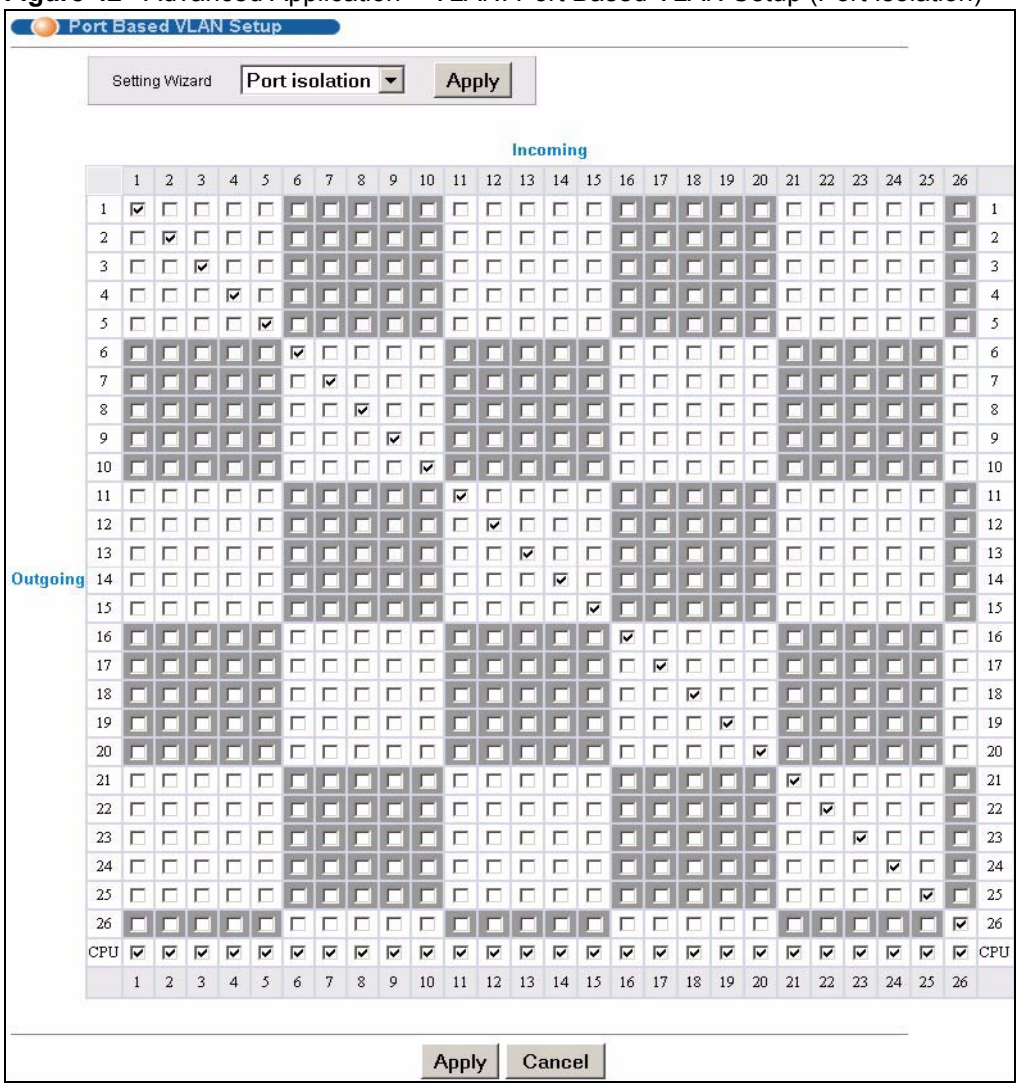
The following screen shows users on a port-based, all-connected VLAN configuration.

Figure 41 Advanced Application > VLAN > Port Based VLAN Setup (All Connected)


Port Based VLAN Setup
Setting Wizard
All connected
Apply
Incoming
Outgoing
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
CPU
Apply
Cancel

The following screen shows users on a port-based, port-isolated VLAN configuration.

Figure 42 Advanced Application > VLAN: Port Based VLAN Setup (Port Isolation)



The following table describes the labels in this screen.

Table 21 Advanced Application > VLAN: Port Based VLAN Setup

LABEL	DESCRIPTION
Setting Wizard	Choose **All connected** or **Port isolation**. **All connected** means all ports can communicate with each other, that is, there are no virtual LANs. All incoming and outgoing ports are selected. This option is the most flexible but also the least secure. **Port isolation** means that each port can only communicate with the CPU management port and cannot communicate with each other. All incoming ports are selected while only the CPU outgoing port is selected. This option is the most limiting but also the most secure. After you make your selection, click **Apply** (top right of screen) to display the screens as mentioned above. You can still customize these settings by adding/deleting incoming or outgoing ports, but you must also click **Apply** at the bottom of the screen.
Incoming	These are the ingress ports; an ingress port is an incoming port, that is, a port through which a data packet enters. If you wish to allow two subscriber ports to talk to each other, you must define the ingress port for both ports. The numbers in the top row denote the incoming port for the corresponding port listed on the left (its outgoing port). **CPU** refers to the Switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the Switch cannot be managed from that port.
Outgoing	These are the egress ports. An egress port is an outgoing port, that is, a port through which a data packet leaves. If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. **CPU** refers to the Switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the Switch cannot be managed from that port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

9

Static MAC Forward Setup

Use these screens to configure static MAC address forwarding.

9.1 Overview

This chapter discusses how to configure forwarding rules based on MAC addresses of devices on your network.

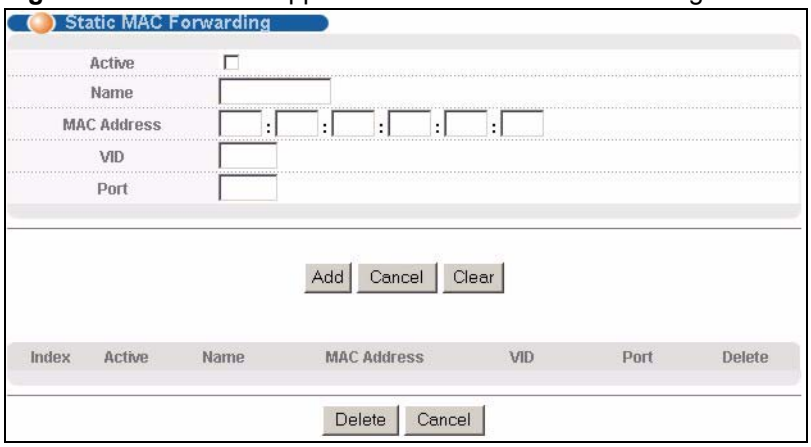
9.2 Configuring Static MAC Forwarding

A static MAC address is an address that has been manually entered in the MAC address table. Static MAC addresses do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port. This may reduce the need for broadcasting.

Static MAC address forwarding together with port security allows only computers in the MAC address table on a port to access the Switch. See Chapter 17 on page 147 for more information on port security.

Click **Advanced Applications > Static MAC Forwarding** in the navigation panel to display the configuration screen as shown.

Figure 43 Advanced Application > Static MAC Forwarding



The following table describes the labels in this screen.

Table 22 Advanced Application > Static MAC Forwarding

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Enter a descriptive name for identification purposes for this static MAC address forwarding rule.
MAC Address	Enter the MAC address in valid MAC address format, that is, six hexadecimal character pairs. Note: Static MAC addresses do not age out.
VID	Enter the VLAN identification number.
Port	Enter the port where the MAC address entered in the previous field will be automatically forwarded.
Add	Click **Add** to save your rule to the Switch's run-time memory. The Switch loses this rule if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	Click an index number to modify a static MAC address rule for a port.
Active	This field displays whether this static MAC address forwarding rule is active (**Yes**) or not (**No**). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for this static MAC address-forwarding rule.
MAC Address	This field displays the MAC address that will be forwarded and the VLAN identification number to which the MAC address belongs.
VID	This field displays the ID number of the VLAN group.
Port	This field displays the port where the MAC address shown in the next field will be forwarded.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

10

Filtering

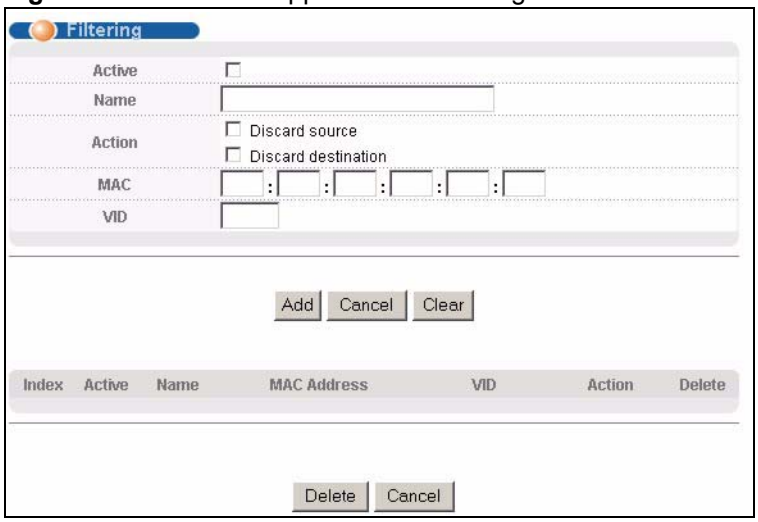
This chapter discusses MAC address port filtering.

10.1 Configure a Filtering Rule

Configure the Switch to filter traffic based on the traffic's source, destination MAC addresses and/or VLAN group (ID).

Click **Advanced Application** > **Filtering** in the navigation panel to display the screen as shown next.

Figure 44 Advanced Application > Filtering



The following table describes the related labels in this screen.

Table 23 Advanced Application > FIltering

LABEL	DESCRIPTION
Active	Make sure to select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by deselecting this check box.
Name	Type a descriptive name (up to 32 printable ASCII characters) for this rule. This is for identification only.

Table 23 Advanced Application > FIltering (continued)

LABEL	DESCRIPTION
Action	Select **Discard source** to drop frames from the source MAC address (specified in the **MAC** field). The Switch can still send frames to the MAC address. Select **Discard destination** to drop frames to the destination MAC address (specified in the **MAC** address). The Switch can still receive frames originating from the MAC address. Select **Discard source** and **Discard destination** to block traffic to/from the MAC address specified in the **MAC** field.
MAC	Type a MAC address in a valid MAC address format, that is, six hexadecimal character pairs.
VID	Type the VLAN group identification number.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to clear the fields to the factory defaults.
Index	This field displays the index number of the rule. Click an index number to change the settings.
Active	This field displays **Yes** when the rule is activated and **No** when is it deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purposes only.
MAC Address	This field displays the source/destination MAC address with the VLAN identification number to which the MAC address belongs.
VID	This field displays the VLAN group identification number.
Delete	Check the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected checkbox(es) in the **Delete** column.

11

Spanning Tree Protocol

The Switch supports Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) as defined in the following standards.

- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1w Rapid Spanning Tree Protocol
- IEEE 802.1s Multiple Spanning Tree Protocol

The Switch also allows you to set up multiple STP configurations (or trees). Ports can then be assigned to the trees.

11.1 STP/RSTP Overview

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a Switch to interact with other (R)STP-compliant switches in your network to ensure that only one path exists between any two stations on the network.

The Switch uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allows faster convergence of the spanning tree than STP (while also being backwards compatible with STP-only aware bridges). In RSTP, topology change information is directly propagated throughout the network from the device that generates the topology change. In STP, a longer delay is required as the device that causes a topology change first notifies the root bridge and then the root bridge notifies the network. Both RSTP and STP flush unwanted learned addresses from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.

In this user's guide, "STP" refers to both STP and RSTP.

11.1.1 STP Terminology

The root bridge is the base of the spanning tree.

Path cost is the cost of transmitting a frame onto a LAN through that port. The recommended cost is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost.

Table 24 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the bridge communicates with the root through the root port. The root port is the port on this Switch with the lowest path cost to the root (the root path cost). If there is no root port, then this Switch has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

11.1.2 How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware switches exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

11.1.3 STP Port States

STP assigns five port states to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

Table 25 STP Port States

PORT STATE	DESCRIPTION
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.

Table 25 STP Port States

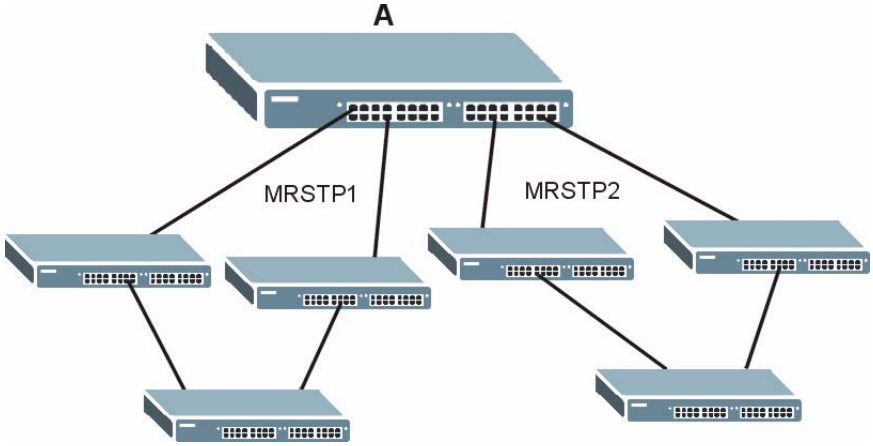
PORT STATE	DESCRIPTION
Listening	All BPDUs are received and processed. Note: The listening state does not exist in RSTP.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

11.1.4 Multiple RSTP

MRSTP (Multiple RSTP) is ZyXEL's proprietary feature that is compatible with RSTP and STP. With MRSTP, you can have more than one spanning tree on your Switch and assign port(s) to each tree. Each spanning tree operates independently with its own bridge information.

In the following example, there are two RSTP instances (**MRSTP 1** and **MRSTP2**) on switch **A**.

Figure 45 MRSTP Network Example



To set up MRSTP, activate MRSTP on the Switch and specify which port(s) belong to which spanning tree.

Each port can belong to one STP tree only.

11.1.5 Multiple STP

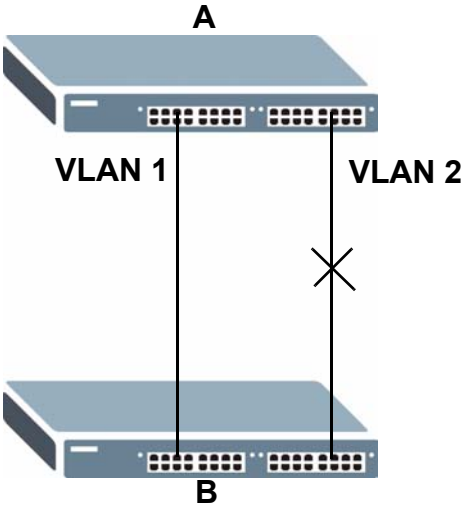
Multiple Spanning Tree Protocol (IEEE 802.1s) is backwards compatible with STP/RSTP and addresses the limitations of existing spanning tree protocols (STP and RSTP) in networks to include the following features:

- One Common and Internal Spanning Tree (CIST) that represents the entire network's connectivity.
- Grouping of multiple bridges (or switching devices) into regions that appear as one single bridge on the network.
- A VLAN can be mapped to a specific Multiple Spanning Tree Instance (MSTI). MSTI allows multiple VLANs to use the same spanning tree.
- Load-balancing is possible as traffic from different VLANs can use distinct paths in a region.

11.1.5.1 MSTP Network Example

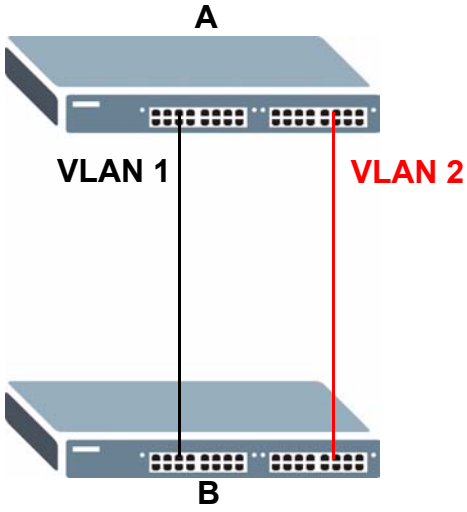
The following figure shows a network example where two VLANs are configured on the two switches. If the switches are using STP or RSTP, the link for VLAN 2 will be blocked as STP and RSTP allow only one link in the network and block the redundant link.

Figure 46 STP/RSTP Network Example



With MSTP, VLANs 1 and 2 are mapped to different spanning trees in the network. Thus traffic from the two VLANs travel on different paths. The following figure shows the network example using MSTP.

Figure 47 MSTP Network Example



11.1.5.2 MST Region

An MST region is a logical grouping of multiple network devices that appears as a single device to the rest of the network. Each MSTP-enabled device can only belong to one MST region. When BPDUs enter an MST region, external path cost (of paths outside this region) is increased by one. Internal path cost (of paths within this region) is increased by one when BPDUs traverse the region.

Devices that belong to the same MST region are configured to have the same MSTP configuration identification settings. These include the following parameters:

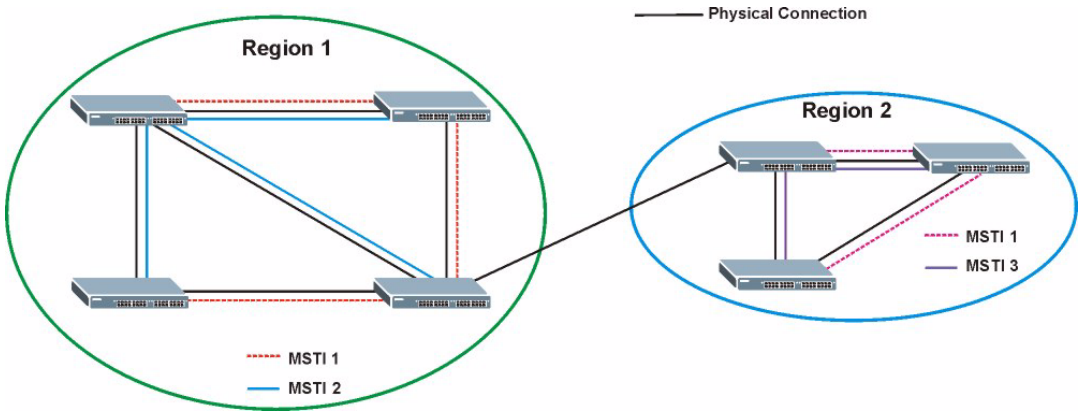
- Name of the MST region
- Revision level as the unique number for the MST region
- VLAN-to-MST Instance mapping

11.1.5.3 MST Instance

An MST Instance (MSTI) is a spanning tree instance. VLANs can be configured to run on a specific MSTI. Each created MSTI is identified by a unique number (known as an MST ID) known internally to a region. Thus an MSTI does not span across MST regions.

The following figure shows an example where there are two MST regions. Regions 1 and 2 have 2 spanning tree instances.

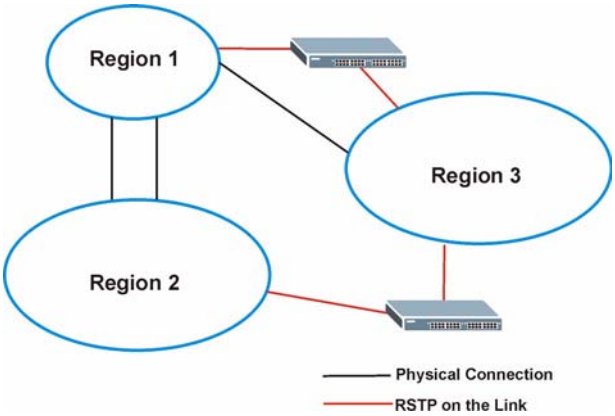
Figure 48 MSTIs in Different Regions



11.1.5.4 Common and Internal Spanning Tree (CIST)

A CIST represents the connectivity of the entire network and it is equivalent to a spanning tree in an STP/RSTP. The CIST is the default MST instance (MSTID 0). Any VLANs that are not members of an MST instance are members of the CIST. In an MSTP-enabled network, there is only one CIST that runs between MST regions and single spanning tree devices. A network may contain multiple MST regions and other network segments running RSTP.

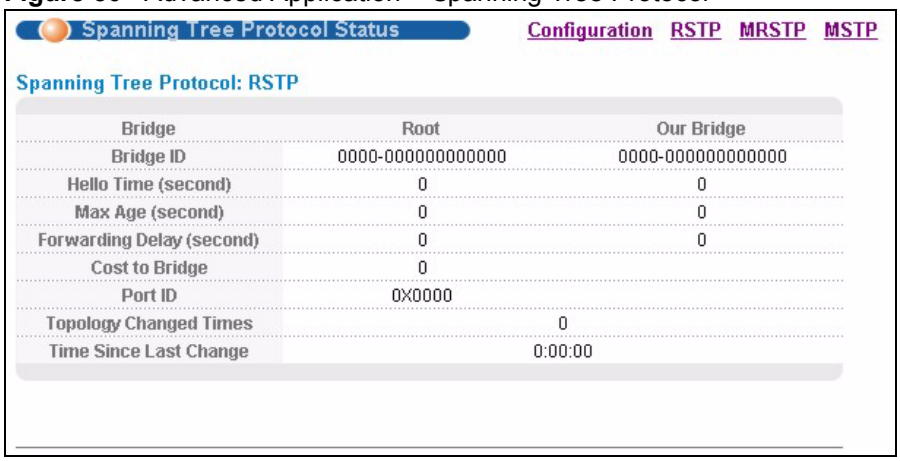
Figure 49 MSTP and Legacy RSTP Network Example



11.2 Spanning Tree Protocol Status Screen

The Spanning Tree Protocol status screen changes depending on what standard you choose to implement on your network. Click **Advanced Application** > **Spanning Tree Protocol** to see the screen as shown.

Figure 50 Advanced Application > Spanning Tree Protocol



This screen differs depending on which STP mode (RSTP, MRSTP or MSTP) you configure on the Switch. This screen is described in detail in the section that follows the configuration section for each STP mode. Click **Configuration** to activate one of the STP standards on the Switch.

11.3 Spanning Tree Configuration

Use the **Spanning Tree Configuration** screen to activate one of the STP modes on the Switch. Click **Configuration** in the **Advanced Application** > **Spanning Tree Protocol**.

Figure 51 Advanced Application > Spanning Tree Protocol > Configuration

The following table describes the labels in this screen.

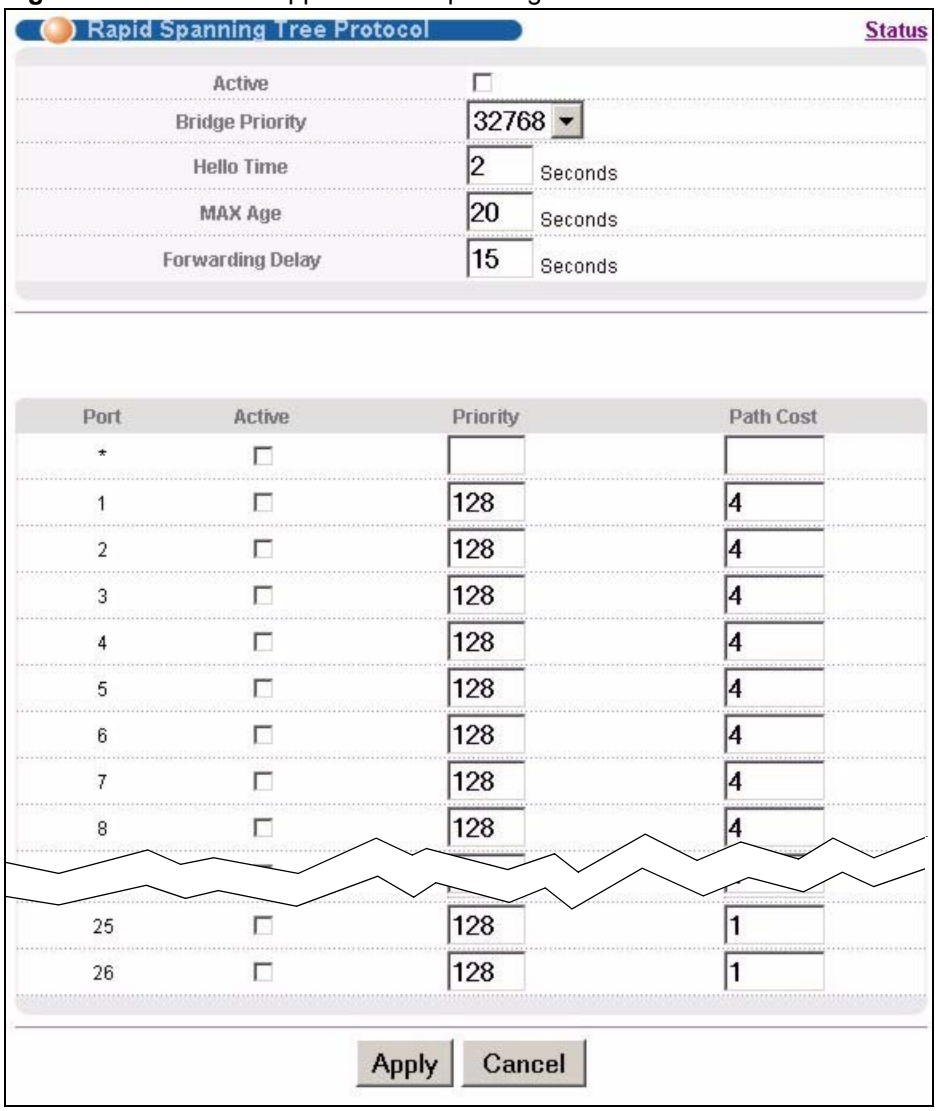
Table 26 Advanced Application > Spanning Tree Protocol > Configuration

LABEL	DESCRIPTION
Spanning Tree Mode	You can activate one of the STP modes on the Switch. Select **Rapid Spanning Tree**, **Multiple Rapid Spanning Tree** or **Multiple Spanning Tree**. See Section 11.1 on page 107 for background information on STP.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11.4 Configure Rapid Spanning Tree Protocol

Use this screen to configure RSTP settings, see Section 11.1 on page 107 for more information on RSTP. Click **RSTP** in the **Advanced Application** > **Spanning Tree Protocol** screen.

Figure 52 Advanced Application > Spanning Tree Protocol > RSTP



The following table describes the labels in this screen.

Table 27 Advanced Application > Spanning Tree Protocol > RSTP

LABEL	DESCRIPTION
Status	Click **Status** to display the **RSTP Status** screen (see Figure 53 on page 116).
Active	Select this check box to activate RSTP. Clear this checkbox to disable RSTP. Note: You must also activate **Rapid Spanning Tree** in the **Advanced Application** > **Spanning Tree Protocol** > **Configuration** screen to enable RSTP on the Switch.

Table 27 Advanced Application > Spanning Tree Protocol > RSTP (continued)

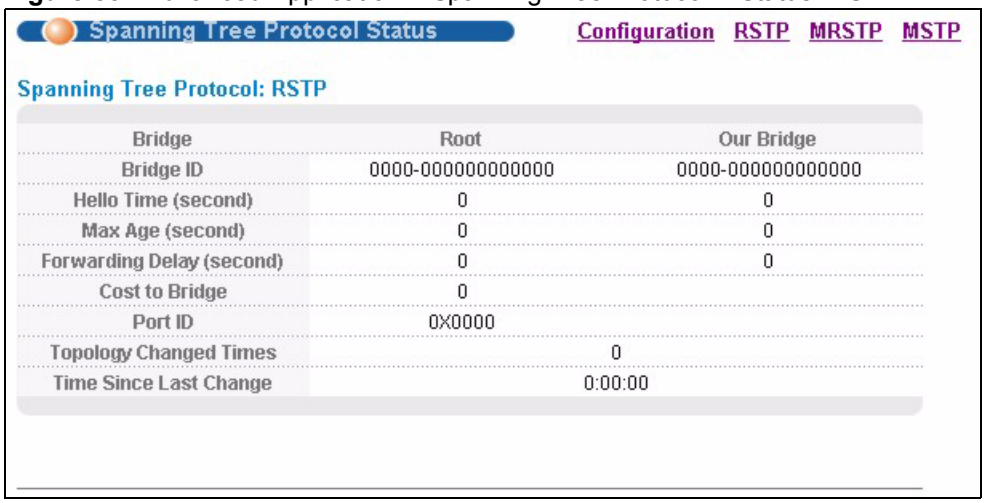
LABEL	DESCRIPTION
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Max Age	This is the maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) a switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: Note: 2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to activate RSTP on this port.
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost - see Table 24 on page 108 for more information.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11.5 Rapid Spanning Tree Protocol Status

Click **Advanced Application** > **Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See Section 11.1 on page 107 for more information on RSTP.

This screen is only available after you activate RSTP on the Switch.

Figure 53 Advanced Application > Spanning Tree Protocol > Status: RSTP



The following table describes the labels in this screen.

Table 28 Advanced Application > Spanning Tree Protocol > Status: RSTP

LABEL	DESCRIPTION
Configuration	Click **Configuration** to specify which STP mode you want to activate. Click **RSTP** to edit RSTP settings on the Switch.
Bridge	**Root** refers to the base of the spanning tree (the root bridge). **Our Bridge** is this Switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of the bridge priority plus the MAC address. This ID is the same for **Root** and **Our Bridge** if the Switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Max Age (second)	This is the maximum time (in seconds) a switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding). See Section 11.1.3 on page 108 for information on port states. Note: The listening state does not exist in RSTP.
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.

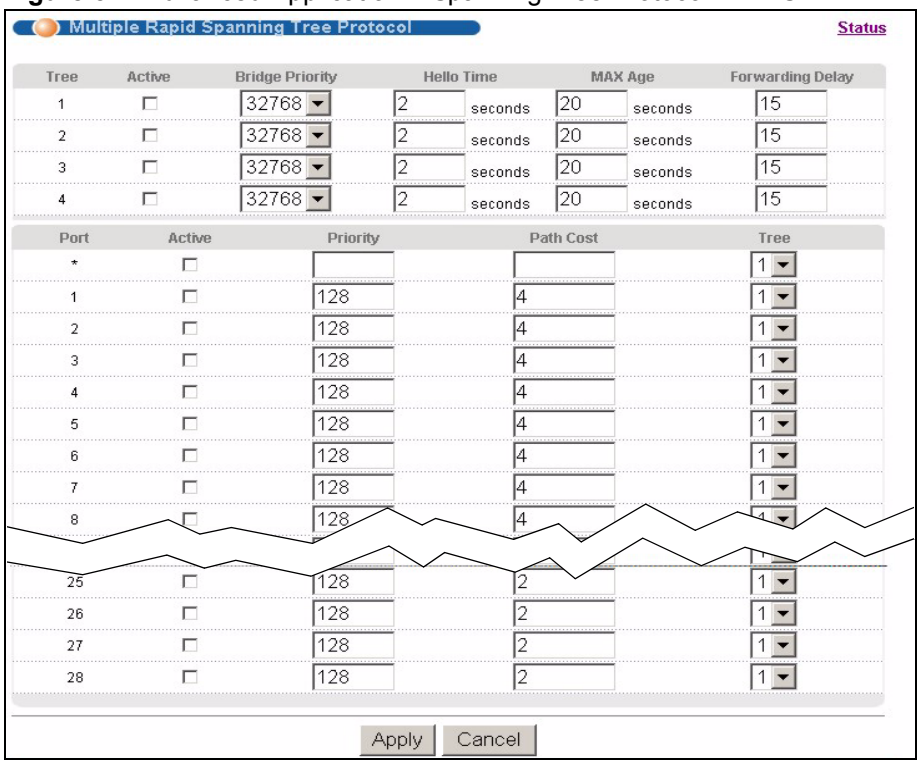
Table 28 Advanced Application > Spanning Tree Protocol > Status: RSTP (continued)

LABEL	DESCRIPTION
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.

11.6 Configure Multiple Rapid Spanning Tree Protocol

To configure MRSTP, click **MRSTP** in the **Advanced Application** > **Spanning Tree Protocol** screen. See Section 11.1 on page 107 for more information on MRSTP.

Figure 54 Advanced Application > Spanning Tree Protocol > MRSTP



The following table describes the labels in this screen.

Table 29 Advanced Application > Spanning Tree Protocol > MRSTP

LABEL	DESCRIPTION
Status	Click **Status** to display the **MRSTP Status** screen (see Figure 53 on page 116).
Tree	This is a read only index number of the STP trees.
Active	Select this check box to activate an STP tree. Clear this checkbox to disable an STP tree. Note: You must also activate **Multiple Rapid Spanning Tree** in the **Advanced Application** > **Spanning Tree Protocol** > **Configuration** screen to enable MRSTP on the Switch.

Table 29 Advanced Application > Spanning Tree Protocol > MRSTP (continued)

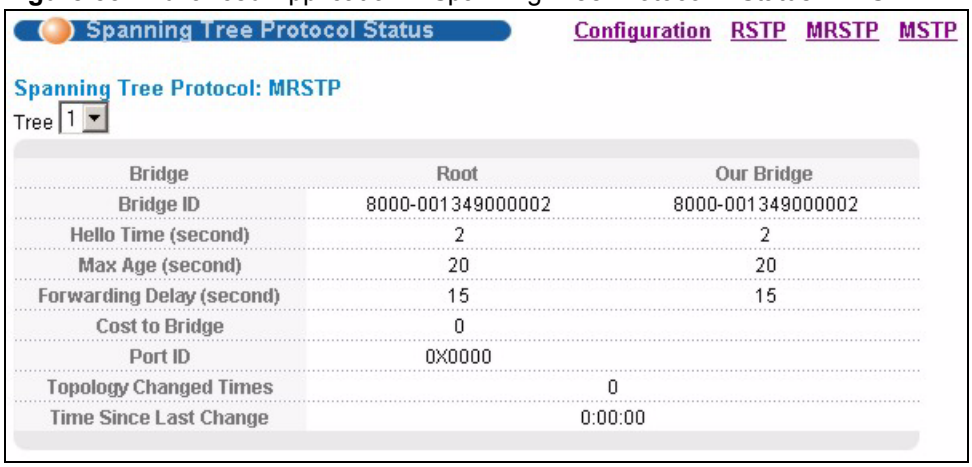
LABEL	DESCRIPTION
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Max Age	This is the maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) a switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: Note: 2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to activate STP on this port.
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in the Switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended that you assign this value according to the speed of the bridge. The slower the media, the higher the cost - see Table 24 on page 108 for more information.
Tree	Select which STP tree configuration this port should participate in.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11.7 Multiple Rapid Spanning Tree Protocol Status

Click **Advanced Application** > **Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See Section 11.1 on page 107 for more information on MRSTP.

This screen is only available after you activate MRSTP on the Switch.

Figure 55 Advanced Application > Spanning Tree Protocol > Status: MRSTP



The following table describes the labels in this screen.

Table 30 Advanced Application > Spanning Tree Protocol > Status: MRSTP

LABEL	DESCRIPTION
Configuration	Click **Configuration** to specify which STP mode you want to activate. Click **MRSTP** to edit MRSTP settings on the Switch.
Tree	Select which STP tree configuration you want to view.
Bridge	**Root** refers to the base of the spanning tree (the root bridge). **Our Bridge** is this Switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for **Root** and **Our Bridge** if the Switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Max Age (second)	This is the maximum time (in seconds) a switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding). Note: The listening state does not exist in RSTP.
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.

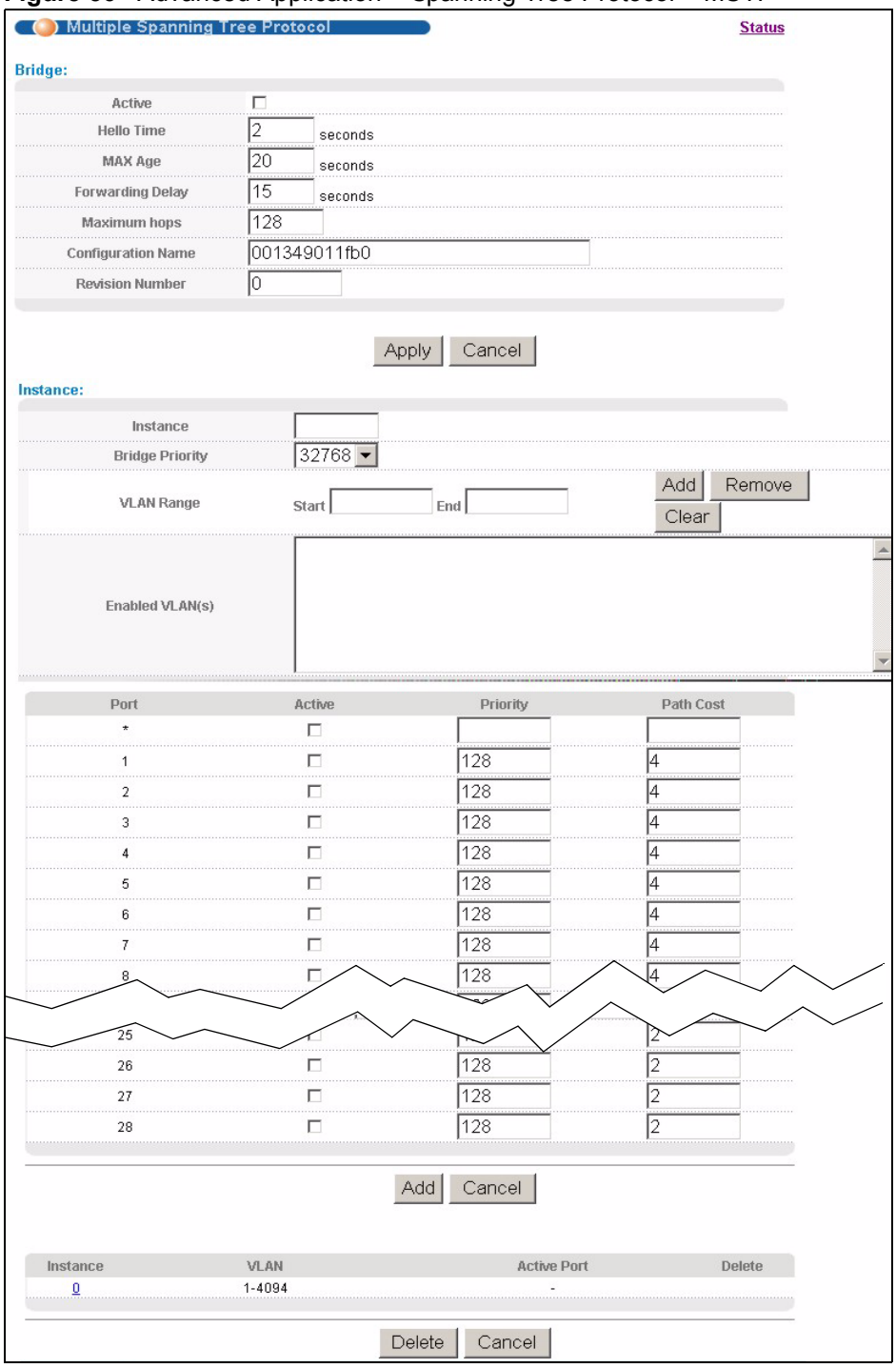
Table 30 Advanced Application > Spanning Tree Protocol > Status: MRSTP (continued)

LABEL	DESCRIPTION
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.

11.8 Configure Multiple Spanning Tree Protocol

To configure MSTP, click **MSTP** in the **Advanced Application** > **Spanning Tree Protocol** screen. See Section 11.1.5 on page 109 for more information on MSTP.

Figure 56 Advanced Application > Spanning Tree Protocol > MSTP



The following table describes the labels in this screen.

Table 31 Advanced Application > Spanning Tree Protocol > MSTP

LABEL	DESCRIPTION
Status	Click **Status** to display the **MSTP Status** screen (see Figure 57 on page 124).
Active	Select this check box to activate MSTP on the Switch. Clear this checkbox to disable MSTP on the Switch. Note: You must also activate **Multiple Spanning Tree** in the **Advanced Application > Spanning Tree Protocol > Configuration** screen to enable MSTP on the Switch.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
MaxAge	This is the maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) a switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: Note: 2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)
Maximum hops	Enter the number of hops (between 1 and 255) in an MSTP region before the BPDU is discarded and the port information is aged.
Configuration Name	Enter a descriptive name (up to 32 characters) of an MST region.
Revision Number	Enter a number to identify a region's configuration. Devices must have the same revision number to belong to the same region.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Instance	Use this section to configure MSTI (Multiple Spanning Tree Instance) settings.
Instance	Enter the number you want to use to identify this MST instance on the Switch. The Switch supports instance numbers 0-16.
Bridge Priority	Set the priority of the Switch for the specific spanning tree instance. The lower the number, the more likely the Switch will be chosen as the root bridge within the spanning tree instance. Enter priority values between 0 and 61440 in increments of 4096 (thus valid values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 and 61440).

Table 31 Advanced Application > Spanning Tree Protocol > MSTP (continued)

LABEL	DESCRIPTION
VLAN Range	Enter the start of the VLAN ID range that you want to add or remove from the VLAN range edit area in the **Start** field. Enter the end of the VLAN ID range that you want to add or remove from the VLAN range edit area in the **End** field. Next click: • **Add** - to add this range of VLAN(s) to be mapped to the MST instance. • **Remove** - to remove this range of VLAN(s) from being mapped to the MST instance. • **Clear** - to remove all VLAN(s) from being mapped to this MST instance.
Enabled VLAN(s)	This field displays which VLAN(s) are mapped to this MST instance.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to add this port to the MST instance.
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in the Switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost - see Table 24 on page 108 for more information.
Add	Click **Add** to save this MST instance to the Switch's run-time memory. The Switch loses this change if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Instance	This field displays the ID of an MST instance.
VLAN	This field displays the VID (or VID ranges) to which the MST instance is mapped.
Active Port	This field display the ports configured to participate in the MST instance.
Delete	Check the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11.9 Multiple Spanning Tree Protocol Status

Click **Advanced Application** > **Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See Section 11.1.5 on page 109 for more information on MSTP.

This screen is only available after you activate MSTP on the Switch.

Figure 57 Advanced Application > Spanning Tree Protocol > Status: MSTP

The following table describes the labels in this screen.

Table 32 Advanced Application > Spanning Tree Protocol > Status: MSTP

LABEL	DESCRIPTION
Configuration	Click **Configuration** to specify which STP mode you want to activate. Click **MSTP** to edit MSTP settings on the Switch.
CST	This section describes the Common Spanning Tree settings.
Bridge	**Root** refers to the base of the spanning tree (the root bridge). **Our Bridge** is this Switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for **Root** and **Our Bridge** if the Switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message.
Max Age (second)	This is the maximum time (in seconds) a switch can wait without receiving a configuration message before attempting to reconfigure.

Table 32 Advanced Application > Spanning Tree Protocol > Status: MSTP (continued)

LABEL	DESCRIPTION
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.
Configuration Name	This field displays the configuration name for this MST region.
Revision Number	This field displays the revision number for this MST region.
Configuration Digest	A configuration digest is generated from the VLAN-MSTI mapping information. This field displays the 16-octet signature that is included in an MSTP BPDU. This field displays the digest when MSTP is activated on the system.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.
Instance:	These fields display the MSTI to VLAN mapping. In other words, which VLANs run on each spanning tree instance.
Instance	This field displays the MSTI ID.
VLAN	This field displays which VLANs are mapped to an MSTI.
MSTI	Select the MST instance settings you want to view.
Bridge	**Root** refers to the base of the MST instance. **Our Bridge** is this Switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for **Root** and **Our Bridge** if the Switch is the root switch.
Internal Cost	This is the path cost from the root port in this MST instance to the regional root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the MST instance.

12

Bandwidth Control

This chapter shows you how you can cap the maximum bandwidth using the **Bandwidth Control** screen.

12.1 Bandwidth Control Overview

Bandwidth control means defining a maximum allowable bandwidth for incoming and/or out-going traffic flows on a port.

12.1.1 CIR and PIR

The Committed Information Rate (CIR) is the guaranteed bandwidth for the incoming traffic flow on a port. The Peak Information Rate (PIR) is the maximum bandwidth allowed for the incoming traffic flow on a port when there is no network congestion.

The CIR and PIR should be set for all ports that use the same uplink bandwidth. If the CIR is reached, packets are sent at the rate up to the PIR. When network congestion occurs, packets through the ingress port exceeding the CIR will be marked for drop.

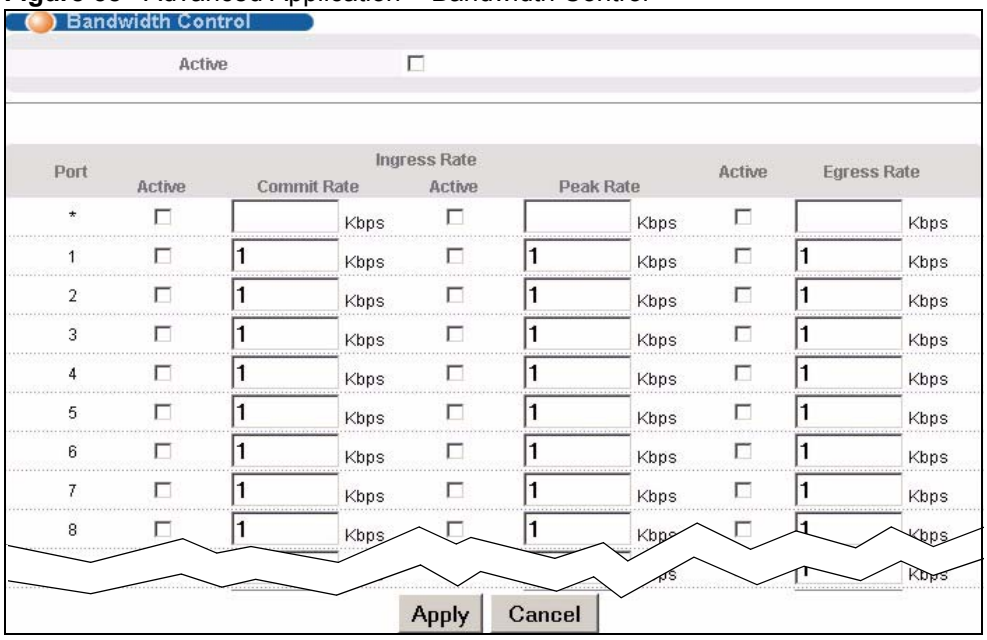
The CIR should be less than the PIR.

The sum of CIRs cannot be greater than or equal to the uplink bandwidth.

12.2 Bandwidth Control Setup

Click **Advanced Application > Bandwidth Control** in the navigation panel to bring up the screen as shown next.

Figure 58 Advanced Application > Bandwidth Control



The following table describes the related labels in this screen.

Table 33 Advanced Application > Bandwidth Control

LABEL	DESCRIPTION
Active	Select this check box to enable bandwidth control on the Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Ingress Rate	
Active	Select this check box to activate commit rate limits on this port.
Commit Rate	Specify the guaranteed bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port. The commit rate should be less than the peak rate. The sum of commit rates cannot be greater than or equal to the uplink bandwidth.
Active	Select this check box to activate peak rate limits on this port.
Peak Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port.
Active	Select this check box to activate egress rate limits on this port.
Egress Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the out-going traffic flow on a port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

13

Broadcast Storm Control

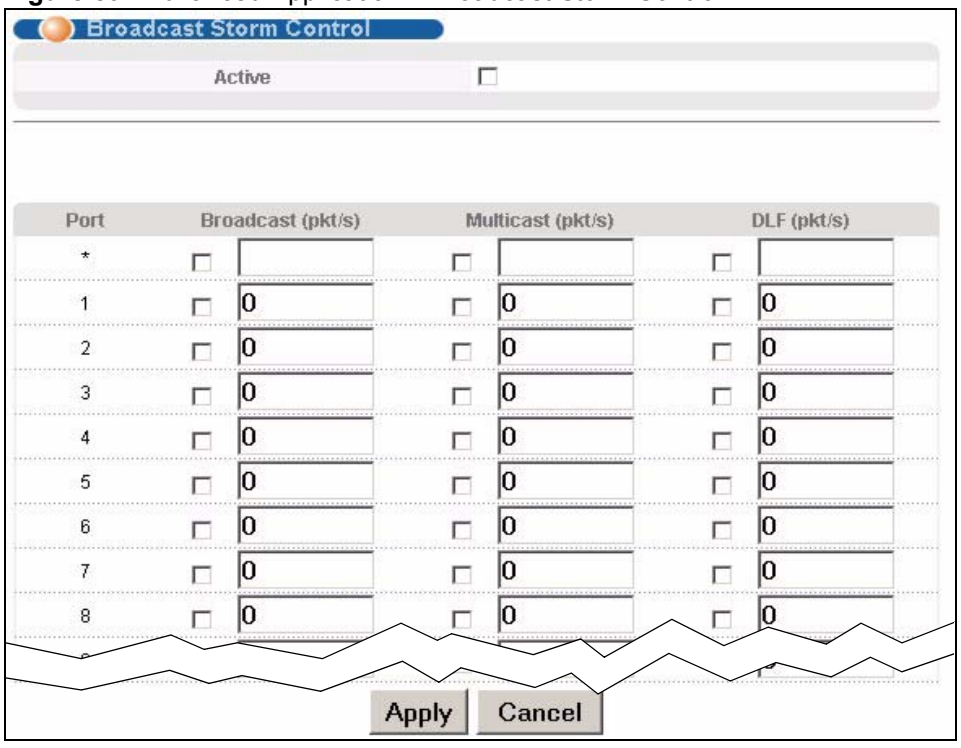
This chapter introduces and shows you how to configure the broadcast storm control feature.

13.1 Broadcast Storm Control Setup

Broadcast storm control limits the number of broadcast, multicast and destination lookup failure (DLF) packets the Switch receives per second on the ports. When the maximum number of allowable broadcast, multicast and/or DLF packets is reached per second, the subsequent packets are discarded. Enable this feature to reduce broadcast, multicast and/or DLF packets in your network. You can specify limits for each packet type on each port.

Click **Advanced Application** > **Broadcast Storm Control** in the navigation panel to display the screen as shown next.

Figure 59 Advanced Application > Broadcast Storm Control



The following table describes the labels in this screen.

Table 34 Advanced Application > Broadcast Storm Control

LABEL	DESCRIPTION
Active	Select this check box to enable traffic storm control on the Switch. Clear this check box to disable this feature.
Port	This field displays a port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Broadcast (pkt/s)	Select this option and specify how many broadcast packets the port receives per second.
Multicast (pkt/s)	Select this option and specify how many multicast packets the port receives per second.
DLF (pkt/s)	Select this option and specify how many destination lookup failure (DLF) packets the port receives per second.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

14 Mirroring

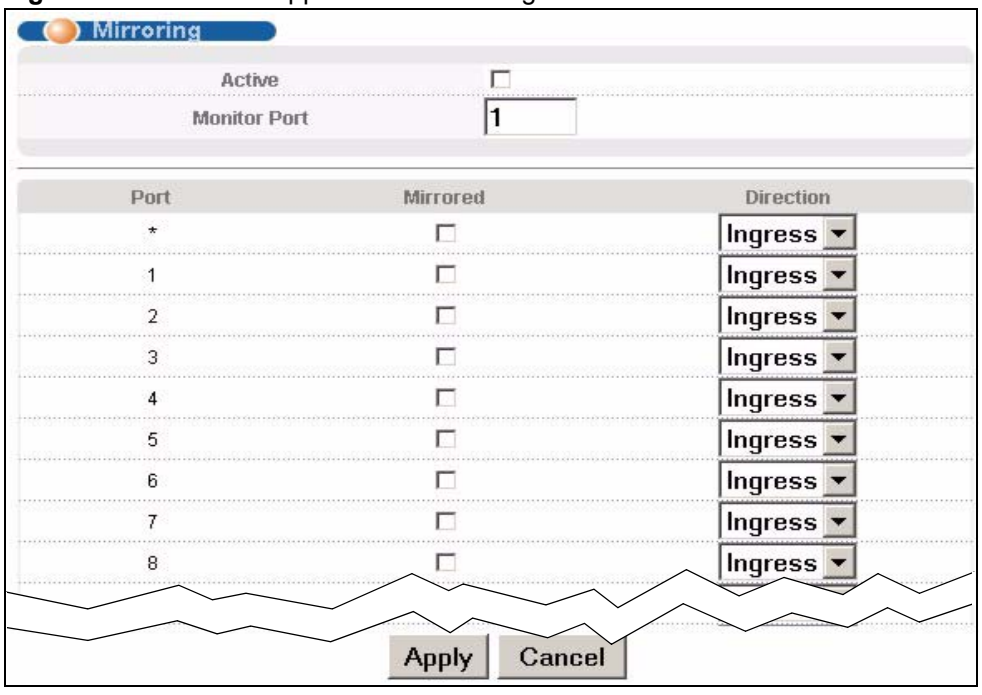
This chapter discusses port mirroring setup screens.

14.1 Port Mirroring Setup

Port mirroring allows you to copy a traffic flow to a monitor port (the port you copy the traffic to) in order that you can examine the traffic from the monitor port without interference.

Click **Advanced Application** > **Mirroring** in the navigation panel to display the **Mirroring** screen. Use this screen to select a monitor port and specify the traffic flow to be copied to the monitor port.

Figure 60 Advanced Application > Mirroring



The following table describes the labels in this screen.

Table 35 Advanced Application > Mirroring

LABEL	DESCRIPTION
Active	Select this check box to activate port mirroring on the Switch. Clear this check box to disable the feature.
Monitor Port	The monitor port is the port you copy the traffic to in order to examine it in more detail without interfering with the traffic flow on the original port(s). Type the port number of the monitor port.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Mirrored	Select this option to mirror the traffic on a port.
Direction	Specify the direction of the traffic to mirror by selecting from the drop-down list box. Choices are **Egress** (outgoing), **Ingress** (incoming) and **Both**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

15

Link Aggregation

This chapter shows you how to logically aggregate physical links to form one logical, higher-bandwidth link.

15.1 Link Aggregation Overview

Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.

However, the more ports you aggregate then the fewer available ports you have. A trunk group is one logical link containing multiple ports.

The beginning port of each trunk group must be physically connected to form a trunk group.

The Switch supports both static and dynamic link aggregation.

In a properly planned network, it is recommended to implement static link aggregation only. This ensures increased network stability and control over the trunk groups on your Switch.

See Section 15.6 on page 138 for a static port trunking example.

15.2 Dynamic Link Aggregation

The Switch adheres to the IEEE 802.3ad standard for static and dynamic (LACP) port trunking.

The Switch supports the link aggregation IEEE802.3ad standard. This standard describes the Link Aggregation Control Protocol (LACP), which is a protocol that dynamically creates and manages trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an operational port fails, then one of the “standby” ports become operational without user intervention. Please note that:

- You must connect all ports point-to-point to the same Ethernet switch and configure the ports for LACP trunking.
- LACP only works on full-duplex links.
- All ports in the same trunk group must have the same media type, speed, duplex mode and flow control settings.

Configure trunk groups or LACP before you connect the Ethernet switch to avoid causing network topology loops.

15.2.1 Link Aggregation ID

LACP aggregation ID consists of the following information[1]:

Table 36 Link Aggregation ID: Local Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00-00	0000	00	0000

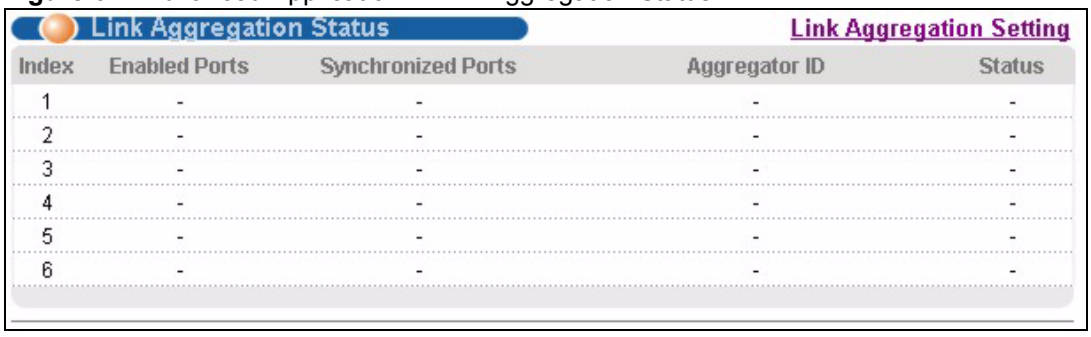
Table 37 Link Aggregation ID: Peer Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00-00	0000	00	0000

15.3 Link Aggregation Status

Click **Advanced Application** > **Link Aggregation** in the navigation panel. The **Link Aggregation Status** screen displays by default. See Section 15.1 on page 133 for more information.

Figure 61 Advanced Application > Link Aggregation Status



The following table describes the labels in this screen.

Table 38 Advanced Application > Link Aggregation Status

LABEL	DESCRIPTION
Index	This field displays the trunk ID to identify a trunk group, that is, one logical link containing multiple ports.
Enabled Port	These are the ports you have configured in the **Link Aggregation** screen to be in the trunk group.

1. Port Priority and Port Number are 0 as it is the aggregator ID for the trunk group, not the individual port.

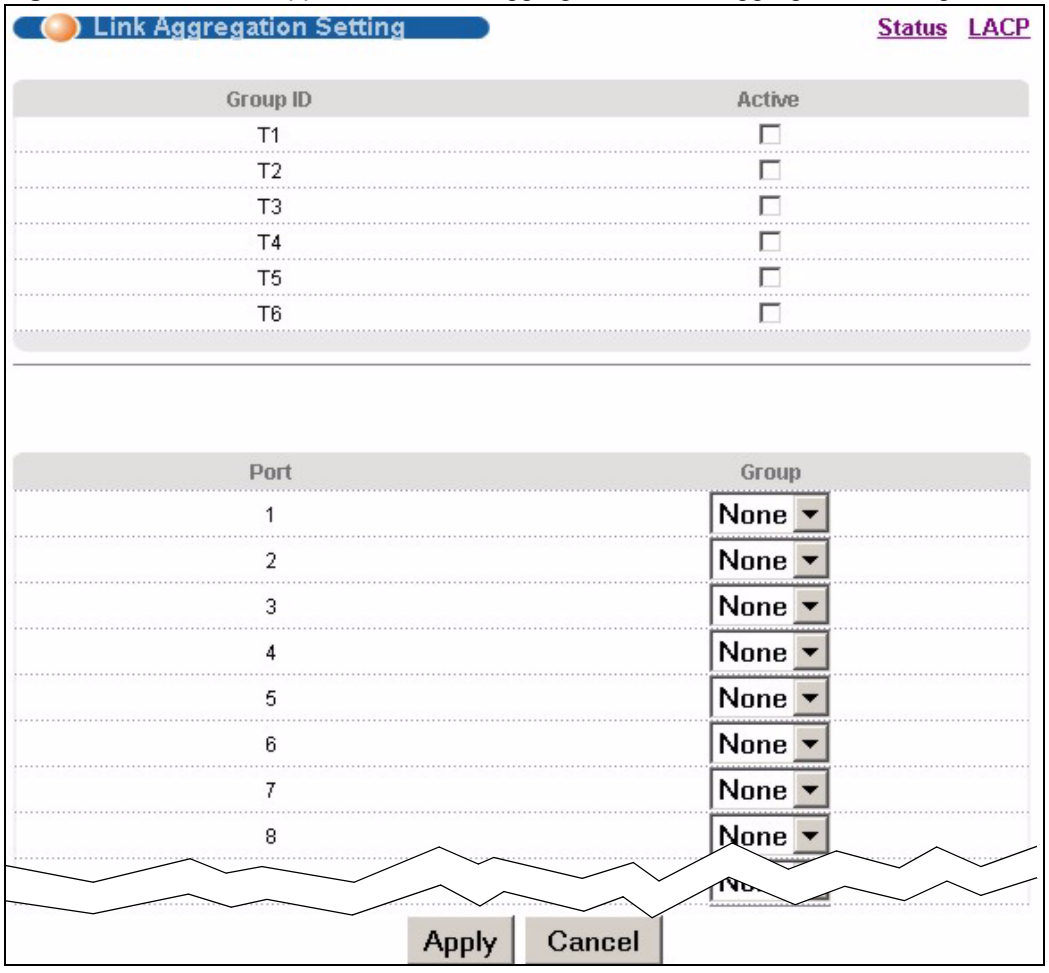
Table 38 Advanced Application > Link Aggregation Status (continued)

LABEL	DESCRIPTION
Synchronized Ports	These are the ports that are currently transmitting data as one logical link in this trunk group.
Aggregator ID	Link Aggregator ID consists of the following: system priority, MAC address, key, port priority and port number. Refer to Section 15.2.1 on page 134 for more information on this field.
Status	This field displays how these ports were added to the trunk group. It displays: • **Static** - if the ports are configured as static members of a trunk group. • **LACP** - if the ports are configured to join a trunk group via LACP.

15.4 Link Aggregation Setting

Click **Advanced Application** > **Link Aggregation > Link Aggregation Setting** to display the screen shown next. See Section 15.1 on page 133 for more information on link aggregation.

Figure 62 Advanced Application > Link Aggregation > Link Aggregation Setting



The following table describes the labels in this screen.

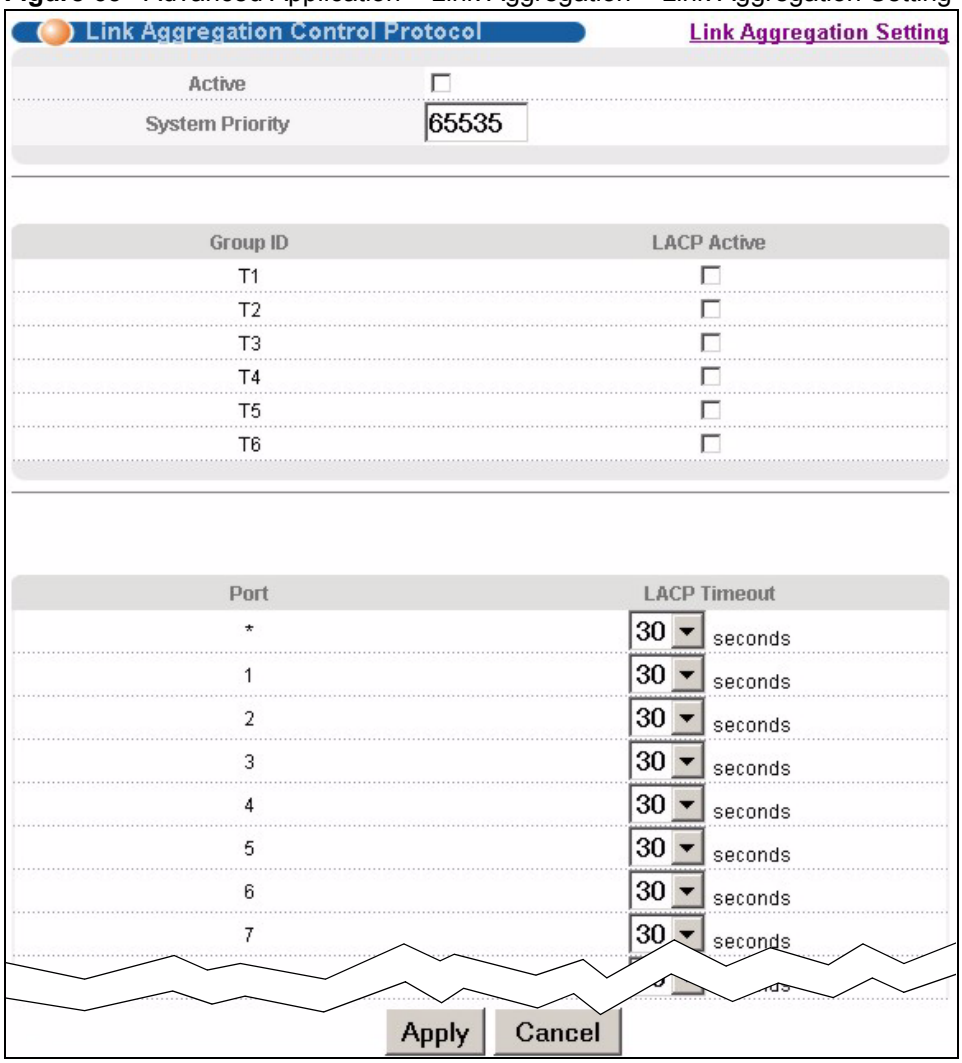
Table 39 Advanced Application > Link Aggregation > Link Aggregation Setting

LABEL	DESCRIPTION
Link Aggregation Setting	This is the only screen you need to configure to enable static link aggregation.
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.
Active	Select this option to activate a trunk group.
Port	This field displays the port number.
Group	Select the trunk group to which a port belongs.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

15.5 Link Aggregation Control Protocol

Click in the **Advanced Application** > **Link Aggregation** > **Link Aggregation Setting** > **LACP** to display the screen shown next. See Section 15.2 on page 133 for more information on dynamic link aggregation.

Figure 63 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP



The following table describes the labels in this screen.

Table 40 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP

LABEL	DESCRIPTION
Link Aggregation Control Protocol	Note: Do not configure this screen unless you want to enable dynamic link aggregation.
Active	Select this checkbox to enable Link Aggregation Control Protocol (LACP).
System Priority	LACP system priority is a number between 1 and 65,535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP “server”. The LACP “server” controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP). The smaller the number, the higher the priority level.
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.
LACP Active	Select this option to enable LACP for a trunk.
Port	This field displays the port number.

Table 40 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP

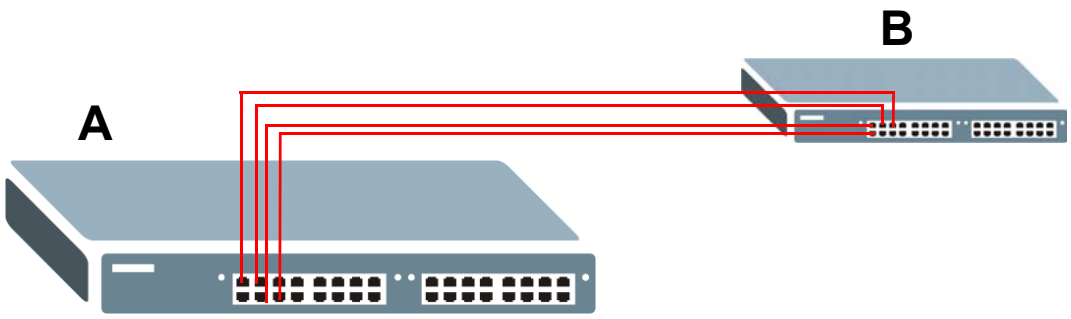
LABEL	DESCRIPTION
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
LACP Timeout	Timeout is the time interval between the individual port exchanges of LACP packets in order to check that the peer port in the trunk group is still up. If a port does not respond after three tries, then it is deemed to be “down” and is removed from the trunk. Set a short timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible. Select either 1 second or 30 seconds.
Apply	Click **Apply** to save your changes to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

15.6 Static Trunking Example

This example shows you how to create a static port trunk group for ports 2-5.

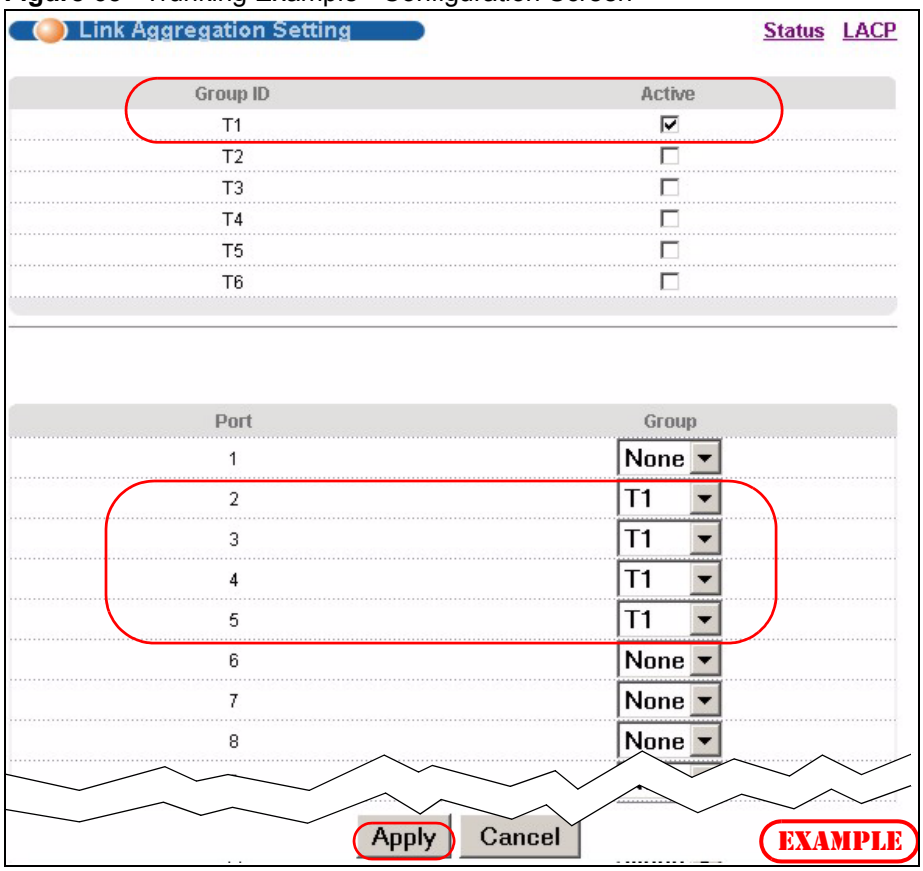
1 **Make your physical connections** - make sure that the ports that you want to belong to the trunk group are connected to the same destination. The following figure shows ports 2-5 on switch **A** connected to switch **B**.

Figure 64 Trunking Example - Physical Connections



2 **Configure static trunking** - Click **Advanced Application** > **Link Aggregation** > **Link Aggregation Setting**. In this screen activate trunking group **T1** and select the ports that should belong to this group as shown in the figure below. Click **Apply** when you are done.

Figure 65 Trunking Example - Configuration Screen



Your trunk group 1 (**T1**) configuration is now complete; you do not need to go to any additional screens.

16

Port Authentication

This chapter describes the IEEE 802.1x and MAC authentication methods.

16.1 Port Authentication Overview

Port authentication is a way to validate access to ports on the Switch to clients based on an external server (authentication server). The Switch supports the following methods for port authentication:

- **IEEE 802.1x**[2] - An authentication server validates access to a port based on a username and password provided by the user.
- **MAC** - An authentication server validates access to a port based on the MAC address and password of the client.

Both types of authentication use the RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) protocol to validate users. See Section 23.1.2 on page 188 for more information on configuring your RADIUS server settings.

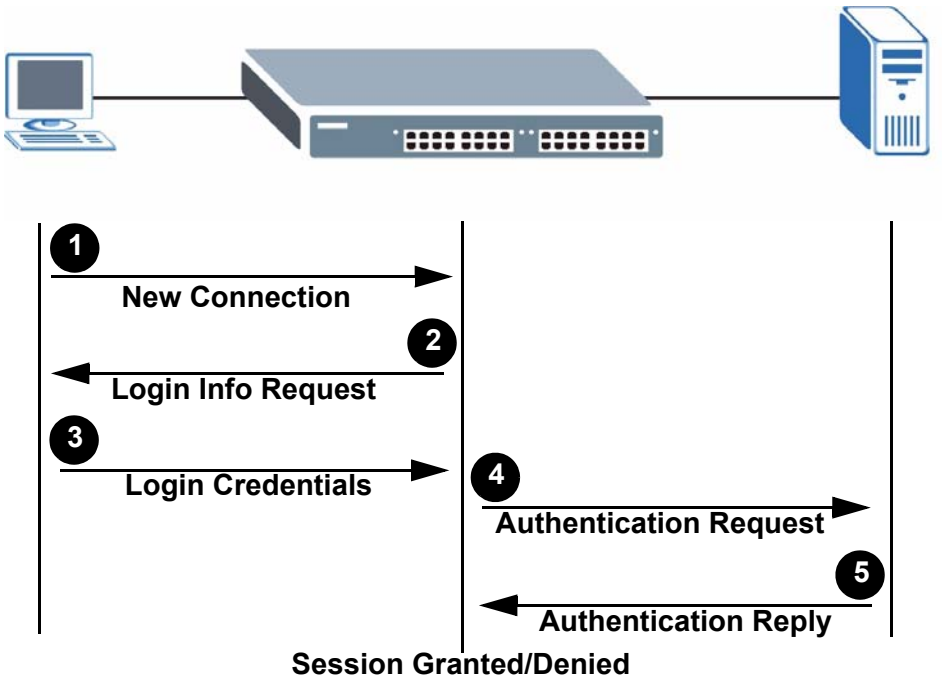
If you enable IEEE 802.1x authentication and MAC authentication on the same port, the Switch performs IEEE 802.1x authentication first. If a user fails to authenticate via the IEEE 802.1x method, then access to the port is denied.

16.1.1 IEEE 802.1x Authentication

The following figure illustrates how a client connecting to a IEEE 802.1x authentication enabled port goes through a validation process. The Switch prompts the client for login information in the form of a user name and password. When the client provides the login credentials, the Switch sends an authentication request to a RADIUS server. The RADIUS server validates whether this client is allowed access to the port.

2. At the time of writing, IEEE 802.1x is not supported by all operating systems. See your operating system documentation. If your operating system does not support 802.1x, then you may need to install 802.1x client software.

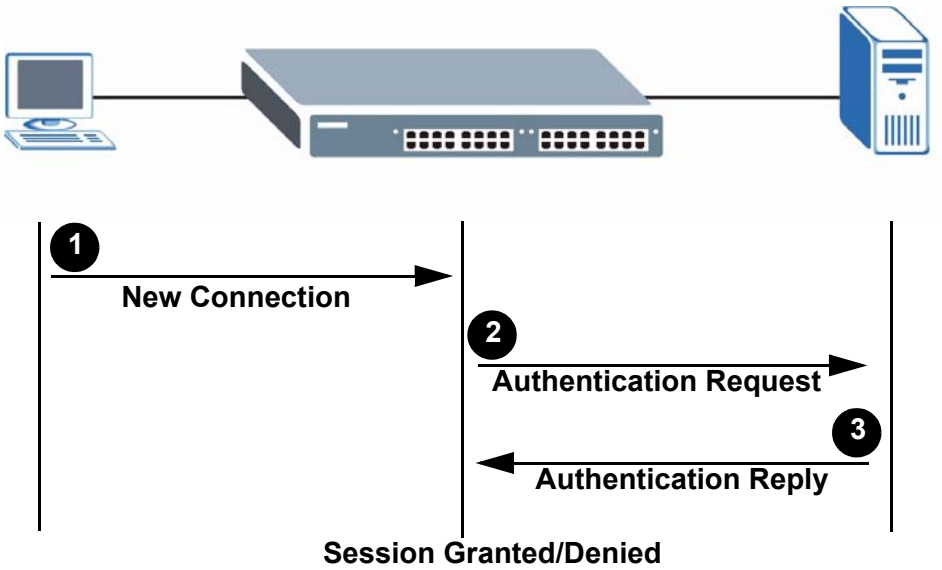
Figure 66 IEEE 802.1x Authentication Process



16.1.2 MAC Authentication

MAC authentication works in a very similar way to IEEE 802.1x authentication. The main difference is that the Switch does not prompt the client for login credentials. The login credentials are based on the source MAC address of the client connecting to a port on the Switch along with a password configured specifically for MAC authentication on the Switch.

Figure 67 MAC Authentication Process



16.2 Port Authentication Configuration

To enable port authentication, first activate the port authentication method(s) you want to use (both on the Switch and the port(s)), then configure the RADIUS server settings in the **Auth and Acct > Radius Server Setup** screen.

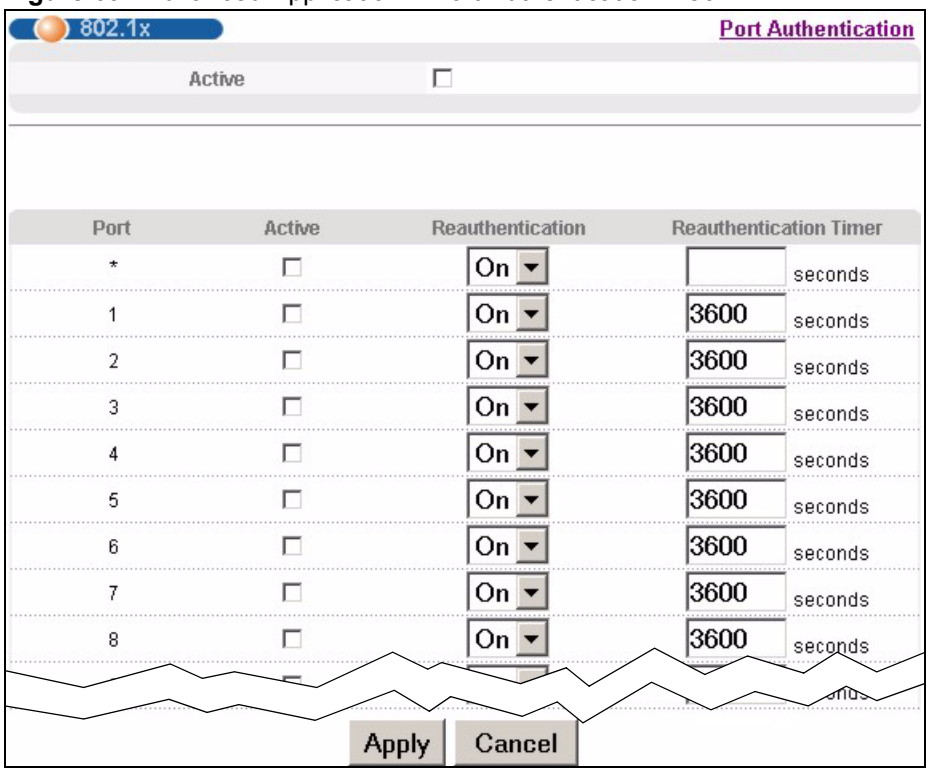
To activate a port authentication method, click **Advanced Application** > **Port Authentication** in the navigation panel. Select a port authentication method in the screen that appears.

Figure 68 Advanced Application > Port Authentication

16.2.1 Activate IEEE 802.1x Security

Use this screen to activate IEEE 802.1x security. In the **Port Authentication** screen click **802.1x** to display the configuration screen as shown.

Figure 69 Advanced Application > Port Authentication > 802.1x



The following table describes the labels in this screen.

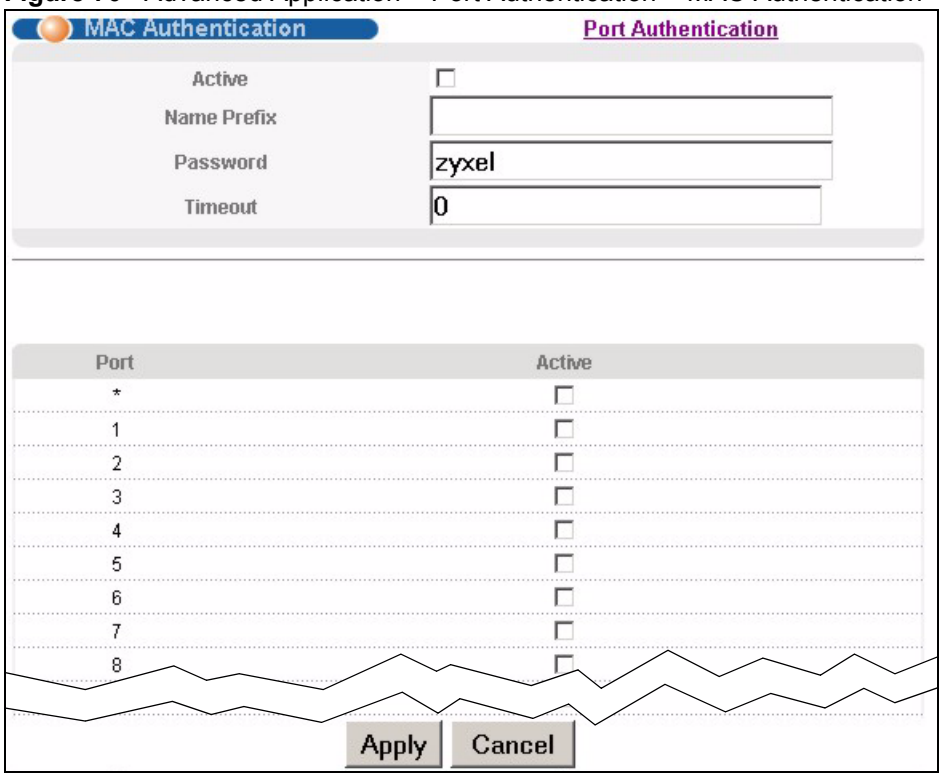
Table 41 Advanced Application > Port Authentication > 802.1x

LABEL	DESCRIPTION
Active	Select this check box to permit 802.1x authentication on the Switch. Note: You must first enable 802.1x authentication on the Switch before configuring it on each port.
Port	This field displays a port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to permit 802.1x authentication on this port. You must first allow 802.1x authentication on the Switch before configuring it on each port.
Reauthentication	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Reauthentication Timer	Specify the length of time required to pass before a client has to re-enter his or her username and password to stay connected to the port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

16.2.2 Activate MAC Authentication

Use this screen to activate MAC authentication. In the **Port Authentication** screen click **MAC Authentication** to display the configuration screen as shown.

Figure 70 Advanced Application > Port Authentication > MAC Authentication



The following table describes the labels in this screen.

Table 42 Advanced Application > Port Authentication > MAC Authentication

LABEL	DESCRIPTION
Active	Select this check box to permit MAC authentication on the Switch. Note: You must first enable MAC authentication on the Switch before configuring it on each port.
Name Prefix	Type the prefix that is appended to all MAC addresses sent to the RADIUS server for authentication. You can enter up to 32 printable ASCII characters. If you leave this field blank, then only the MAC address of the client is forwarded to the RADIUS server.
Password	Type the password the Switch sends along with the MAC address of a client for authentication with the RADIUS server. You can enter up to 32 printable ASCII characters.
Timeout	Specify the amount of time before the Switch allows a client MAC address that fails authentication to try and authenticate again. Maximum time is 3000 seconds. When a client fails MAC authentication, its MAC address is learned by the MAC address table with a status of denied. The timeout period you specify here is the time the MAC address entry stays in the MAC address table until it is cleared. If you specify 0 for the timeout value, then this entry will not be deleted from the MAC address table. Note: If the **Aging Time** in the **Switch Setup** screen is set to a lower value, then it supersedes this setting. See Section 7.5 on page 81.
Port	This field displays a port number.

Table 42 Advanced Application > Port Authentication > MAC Authentication (continued)

LABEL	DESCRIPTION
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to permit MAC authentication on this port. You must first allow MAC authentication on the Switch before configuring it on each port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

17

Port Security

This chapter shows you how to set up port security.

17.1 About Port Security

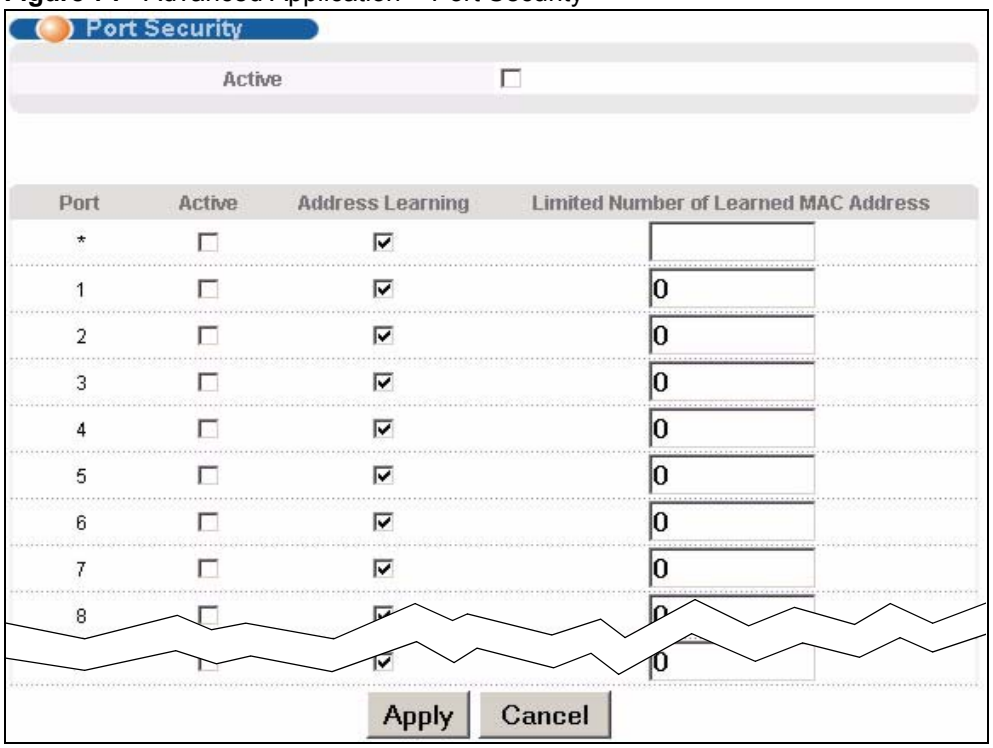
Port security allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the Switch. The Switch can learn up to 16K MAC addresses in total with no limit on individual ports other than the sum cannot exceed 16K.

For maximum port security, enable this feature, disable MAC address learning and configure static MAC address(es) for a port. It is not recommended you disable port security together with MAC address learning as this will result in many broadcasts. By default, MAC address learning is still enabled even though the port security is not activated.

17.2 Port Security Setup

Click **Advanced Application** > **Port Security** in the navigation panel to display the screen as shown.

Figure 71 Advanced Application > Port Security



The following table describes the labels in this screen.

Table 43 Advanced Application > Port Security

LABEL	DESCRIPTION
Active	Select this option to enable port security on the Switch.
Port	This field displays a port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some of the settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable the port security feature on this port. The Switch forwards packets whose MAC address(es) is in the MAC address table on this port. Packets with no matching MAC address(es) are dropped. Clear this check box to disable the port security feature. The Switch forwards all packets on this port.
Address Learning	MAC address learning reduces outgoing broadcast traffic. For MAC address learning to occur on a port, the port itself must be active with address learning enabled.
Limited Number of Learned MAC Address	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device must wait until one of the five learned MAC addresses ages out. MAC address aging out time can be set in the **Switch Setup** screen. The valid range is from “0” to “16384”. “0” means this feature is disabled.

Table 43 Advanced Application > Port Security (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

18

Classifier

This chapter introduces and shows you how to configure the packet classifier on the Switch.

18.1 About the Classifier and QoS

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

Configure QoS on the Switch to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves two separate steps:

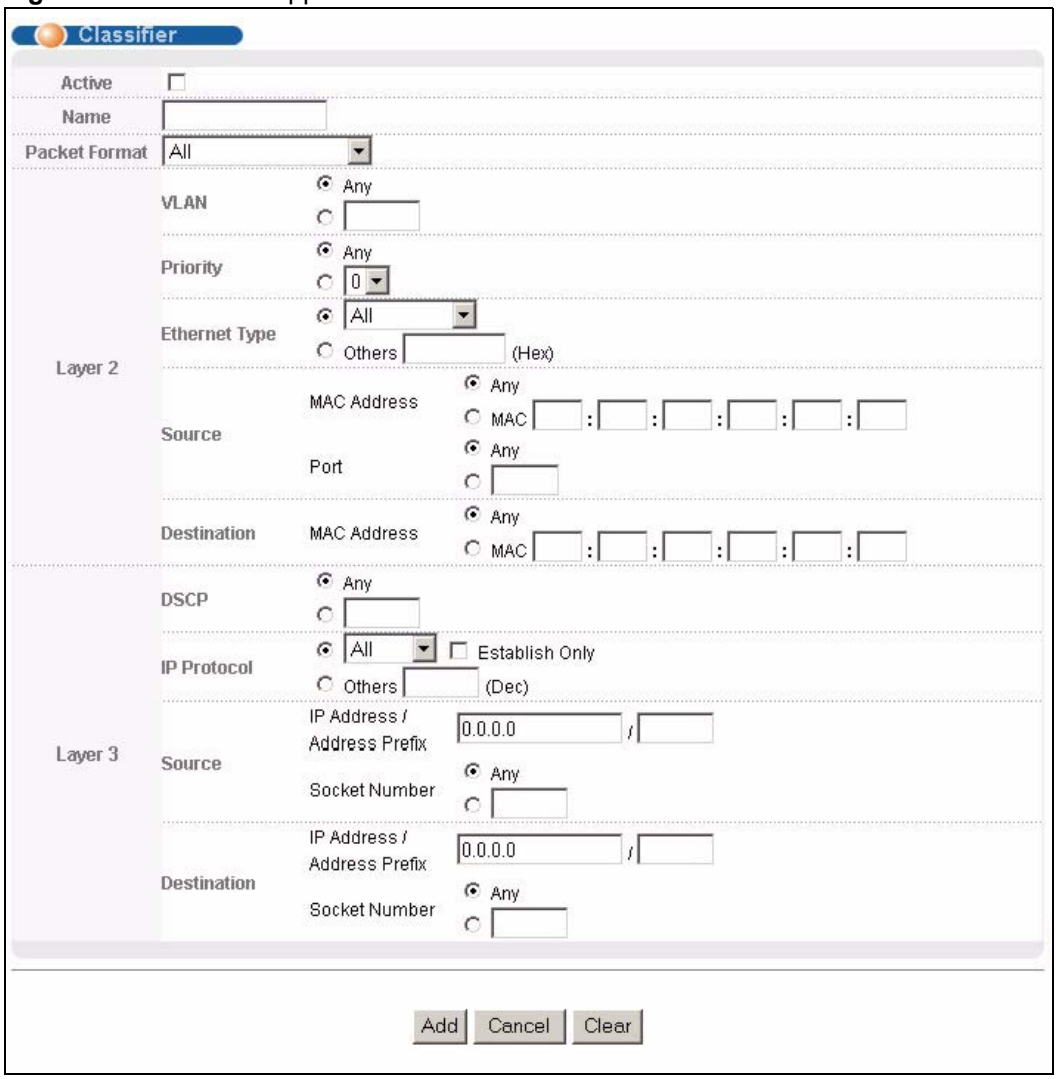
1. Configure classifiers to sort traffic into different flows.
2. Configure policy rules to define actions to be performed for a classified traffic flow (refer to Chapter 19 on page 157 to configure policy rules).

18.2 Configuring the Classifier

Use the **Classifier** screen to define the classifiers. After you define the classifier, you can specify actions (or policy) to act upon the traffic that matches the rules. To configure policy rules, refer to Chapter 19 on page 157.

Click **Advanced Application > Classifier** in the navigation panel to display the configuration screen as shown.

Figure 72 Advanced Application > Classifier



The following table describes the labels in this screen.

Table 44 Advanced Application > Classifier

LABEL	DESCRIPTION
Active	Select this option to enable this rule.
Name	Enter a descriptive name for this rule for identifying purposes.
Packet Format	Specify the format of the packet. Choices are **All**, **802.3 tagged**, **802.3 untagged**, **Ethernet II tagged** and **Ethernet II untagged**. A value of **802.3** indicates that the packets are formatted according to the IEEE 802.3 standards. A value of **Ethernet II** indicates that the packets are formatted according to RFC 894, Ethernet II encapsulation.
Layer 2 Specify the fields below to configure a layer 2 classifier.	
VLAN	Select **Any** to classify traffic from any VLAN or select the second option and specify the source VLAN ID in the field provided.
Priority	Select **Any** to classify traffic from any priority level or select the second option and specify a priority level in the field provided.

Table 44 Advanced Application > Classifier (continued)

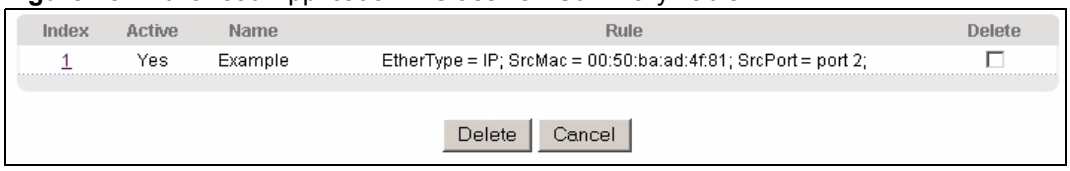
LABEL	DESCRIPTION
Ethernet Type	Select an Ethernet type or select **Other** and enter the Ethernet type number in hexadecimal value. Refer to Table 46 on page 154 for information.
Source	
MAC Address	Select **Any** to apply the rule to all MAC addresses. To specify a source, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs).
Port	Type the port number to which the rule should be applied. You may choose one port only or all ports (**Any**).
Destination	
MAC Address	Select **Any** to apply the rule to all MAC addresses. To specify a destination, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs).
Layer 3 Specify the fields below to configure a layer 3 classifier.	
DSCP	Select **Any** to classify traffic from any DSCP or select the second option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
IP Protocol	Select an IP protocol type or select **Other** and enter the protocol number in decimal value. Refer to Table 47 on page 155 for more information. You may select **Establish Only** for **TCP** protocol type. This means that the Switch will pick out the packets that are sent to establish TCP connections.
Source	
IP Address/ Address Prefix	Enter a source IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Socket Number	Note: You must select either **UDP** or **TCP** in the **IP Protocol** field before you configure the socket numbers. Select **Any** to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Destination	
IP Address/ Address Prefix	Enter a destination IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Socket Number	Note: You must select either **UDP** or **TCP** in the **IP Protocol** field before you configure the socket numbers. Select **Any** to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Add	Click **Add** to insert the entry in the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to set the above fields back to the factory defaults.

18.3 Viewing and Editing Classifier Configuration

To view a summary of the classifier configuration, scroll down to the summary table at the bottom of the **Classifier** screen. To change the settings of a rule, click a number in the **Index** field.

When two rules conflict with each other, a higher layer rule has priority over a lower layer rule.

Figure 73 Advanced Application > Classifier: Summary Table



The following table describes the labels in this screen.

Table 45 Classifier: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of the rule. Click an index number to edit the rule.
Active	This field displays **Yes** when the rule is activated and **No** when it is deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purposes only.
Rule	This field displays a summary of the classifier rule's settings.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

The following table shows some other common Ethernet types and the corresponding protocol number.

Table 46 Common Ethernet Types and Protocol Number

ETHERNET TYPE	PROTOCOL NUMBER
IP ETHII	0800
X.75 Internet	0801
NBS Internet	0802
ECMA Internet	0803
Chaosnet	0804
X.25 Level 3	0805
XNS Compat	0807
Banyan Systems	0BAD
BBN Simnet	5208
IBM SNA	80D5
AppleTalk AARP	80F3

Some of the most common IP ports are:

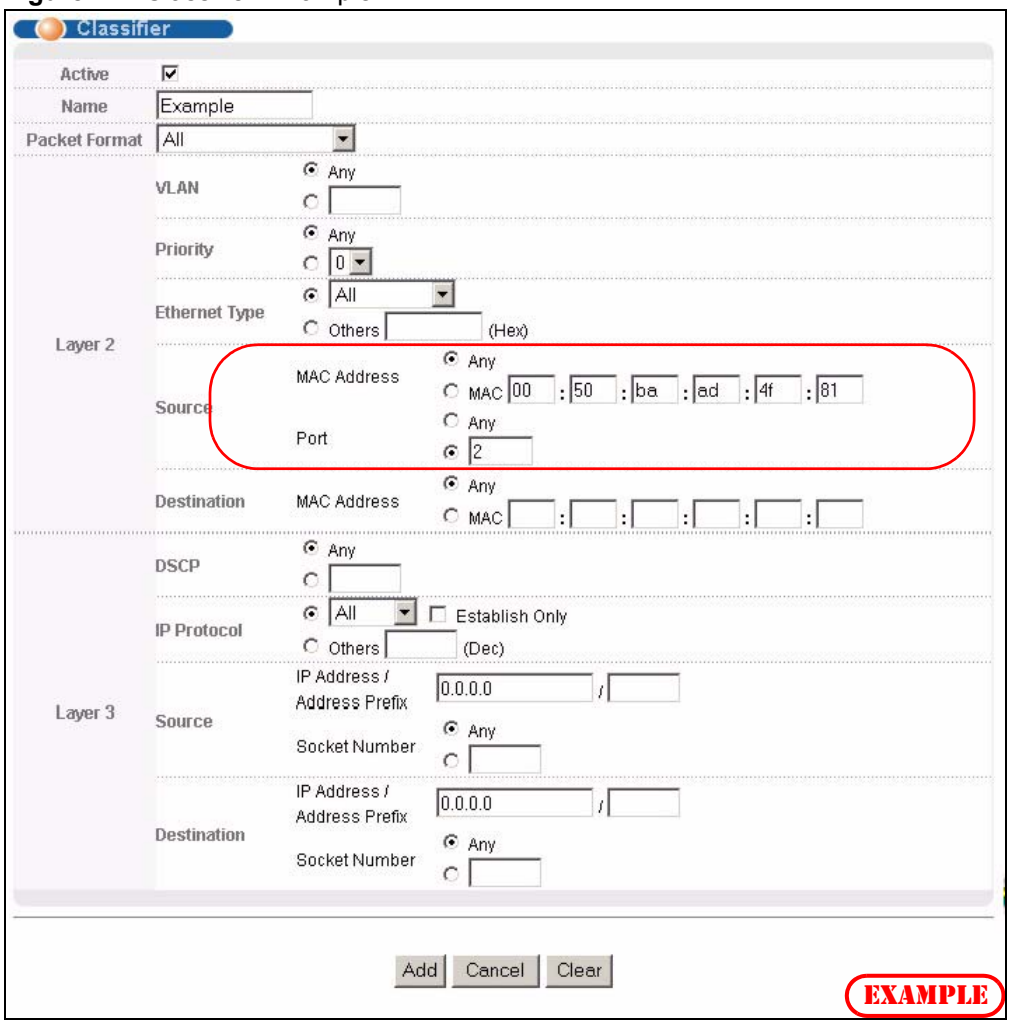
Table 47 Common IP Ports

PORT NUMBER	PORT NAME
21	FTP
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3

18.4 Classifier Example

The following screen shows an example of configuring a classifier that identifies all traffic from MAC address 00:50:ba:ad:4f:81 on port 2.

Figure 74 Classifier: Example



After you have configured a classifier, you can configure a policy to define action(s) on the classified traffic flow. See Chapter 19 on page 157 for information on configuring a policy rule.

19

Policy Rule

This chapter shows you how to configure policy rules.

19.1 Policy Rules Overview

A classifier distinguishes traffic into flows based on the configured criteria (refer to Chapter 18 on page 151 for more information). A policy rule ensures that a traffic flow gets the requested treatment in the network.

19.1.1 DiffServ

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

19.1.2 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

DSCP (6 bits)	Unused (2 bits)

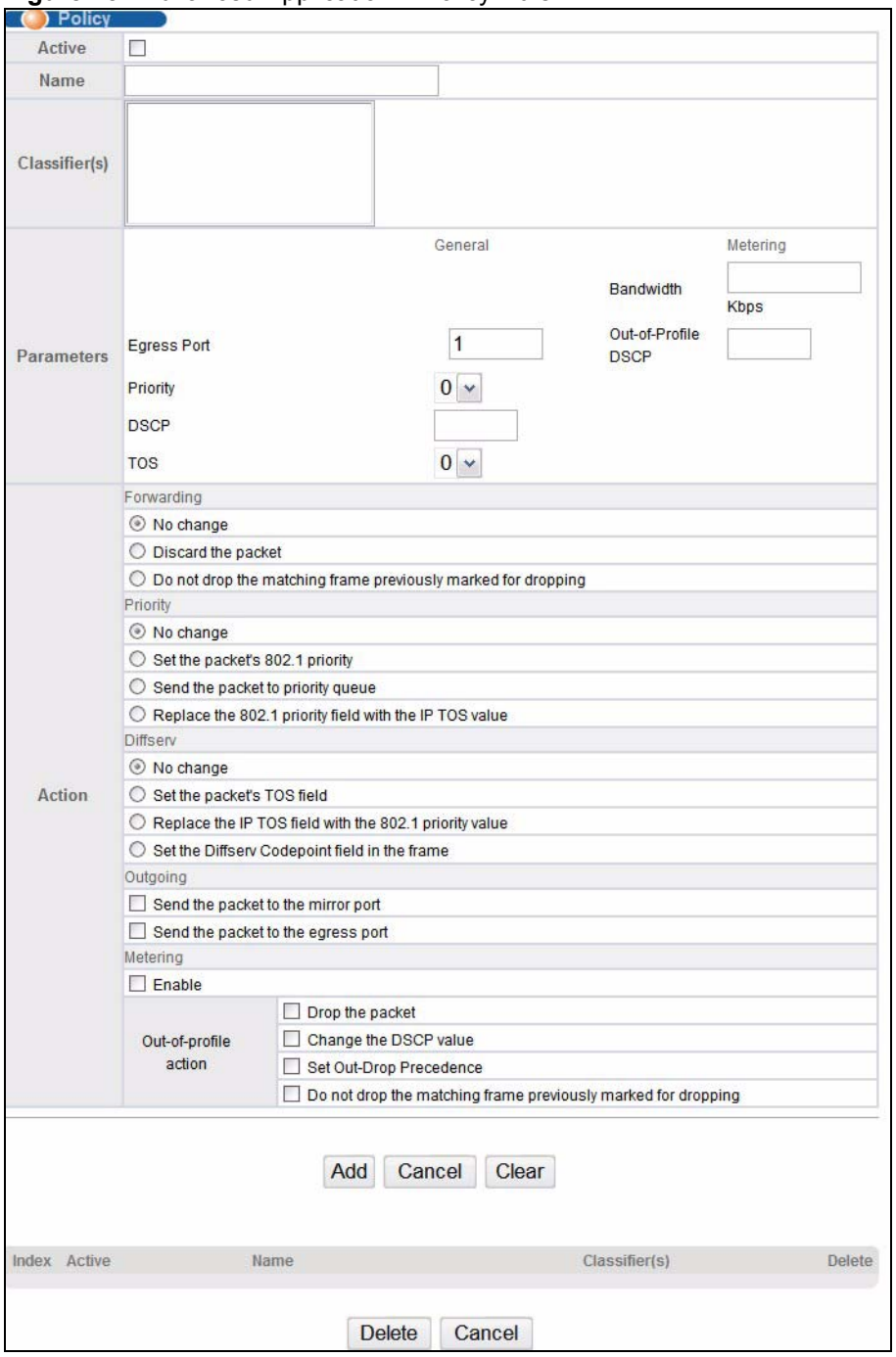
The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

19.2 Configuring Policy Rules

You must first configure a classifier in the **Classifier** screen. Refer to Section 18.2 on page 151 for more information.

Click **Advanced Applications > Policy Rule** in the navigation panel to display the screen as shown.

Figure 75 Advanced Application > Policy Rule



The following table describes the labels in this screen.

Table 48 Advanced Application > Policy Rule

LABEL	DESCRIPTION
Active	Select this option to enable the policy.
Name	Enter a descriptive name for identification purposes.
Classifier(s)	This field displays the active classifier(s) you configure in the **Classifier** screen. Select the classifier(s) to which this policy rule applies. To select more than one classifier, press [SHIFT] and select the choices at the same time.
Parameters Set the fields below for this policy. You only have to set the field(s) that is related to the action(s) you configure in the **Action** field.	
General	
Egress Port	Type the number of an outgoing port.
Priority	Specify a priority level.
DSCP	Specify a DSCP (DiffServ Code Point) number between 0 and 63.
TOS	Specify the type of service (TOS) priority level.
Metering	You can configure the desired bandwidth available to a traffic flow. Traffic that exceeds the maximum bandwidth allocated (in cases where the network is congested) is called out-of-profile traffic.
Bandwidth	Specify the bandwidth in kilobit per second (Kbps). Enter a number between 1 and 1000000.
Out-of-Profile DSCP	Specify a new DSCP number (between 0 and 63) if you want to replace or remark the DSCP number for out-of-profile traffic.
Action Specify the action(s) the Switch takes on the associated classified traffic flow.	
Forwarding	Select **No change** to forward the packets. Select **Discard the packet** to drop the packets. Select **Do not drop the matching frame previously marked for dropping** to retain the frames that were marked to be dropped before.
Priority	Select **No change** to keep the priority setting of the frames. Select **Set the packet's 802.1 priority** to replace the packet's 802.1 priority field with the value you set in the Priority field. Select **Send the packet to priority queue** to put the packets in the designated queue. Select **Replace the 802.1 priority field with the IP TOS value** to replace the packet's 802.1 priority field with the value you set in the **TOS** field.
Diffserv	Select **No change** to keep the TOS and/or DSCP fields in the packets. Select **Set the packet's TOS field** to set the TOS field with the value you configure in the **TOS** field. Select **Replace the IP TOS with the 802.1 priority value** to replace the TOS field with the value you configure in the **Priority** field. Select **Set the Diffserv Codepoint field in the frame** to set the DSCP field with the value you configure in the **DSCP** field.
Outgoing	Select **Send the packet to the mirror port** to send the packet to the mirror port. Select **Send the packet to the egress port** to send the packet to the egress port.
Metering	Select **Enable** to activate bandwidth limitation on the traffic flow(s) then set the actions to be taken on out-of-profile packets.

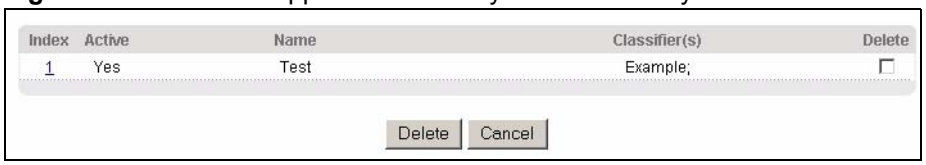
Table 48 Advanced Application > Policy Rule (continued)

LABEL	DESCRIPTION
Out-of-profile action	Select the action(s) to be performed for out-of-profile traffic. Select **Drop the packet** to discard the out-of-profile traffic. Select **Change the DSCP value** to replace the DSCP field with the value specified in the **Out of profile DSCP** field. Select **Set Out-Drop Precedence** to mark out-of-profile traffic and drop it when network is congested. Select **Do not drop the matching frame previously marked for dropping** to queue the frames that are marked to be dropped.
Add	Click **Add** to insert the entry in the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to set the above fields back to the factory defaults.

19.3 Viewing and Editing Policy Configuration

To view a summary of the classifier configuration, scroll down to the summary table at the bottom of the **Policy** screen. To change the settings of a rule, click a number in the **Index** field.

Figure 76 Advanced Application > Policy Rule: Summary Table



The following table describes the labels in this screen.

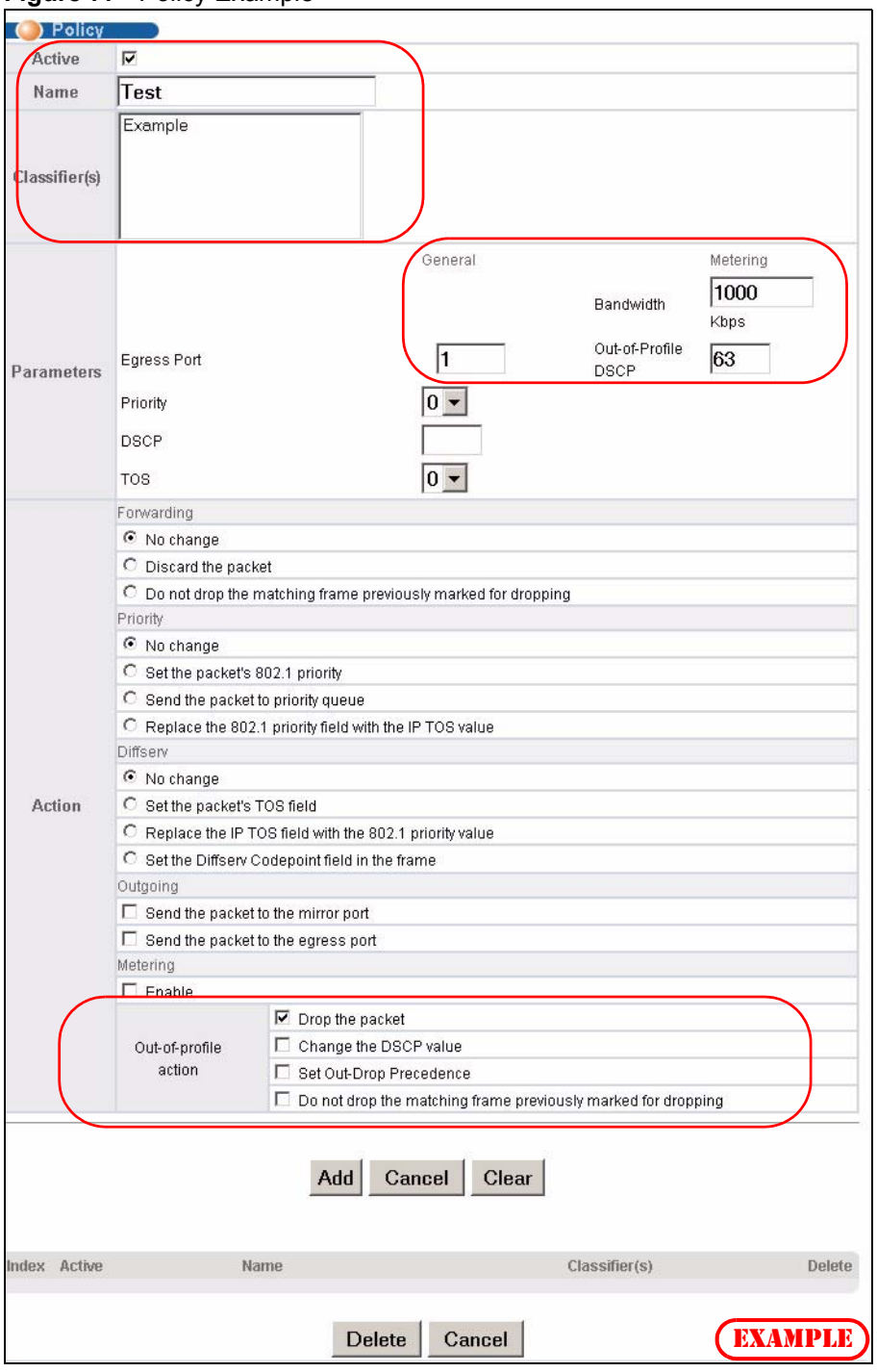
Table 49 Policy: Summary Table

LABEL	DESCRIPTION
Index	This field displays the policy index number. Click an index number to edit the policy.
Active	This field displays **Yes** when policy is activated and **No** when is it deactivated.
Name	This field displays the name you have assigned to this policy.
Classifier(s)	This field displays the name(s) of the classifier to which this policy applies.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

19.4 Policy Example

The figure below shows an example **Policy** screen where you configure a policy to limit bandwidth and discard out-of-profile traffic on a traffic flow classified using the **Example** classifier (refer to Section 18.4 on page 155).

Figure 77 Policy Example



20

Queuing Method

This chapter introduces the queuing methods supported.

20.1 Queuing Method Overview

Queuing is used to help solve performance degradation when there is network congestion. Use the **Queuing Method** screen to configure queuing algorithms for outgoing traffic. See also **Priority Queue Assignment** in **Switch Setup** and **802.1p Priority** in **Port Setup** for related information.

Queuing algorithms allow switches to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.

20.1.1 Strictly Priority

Strictly Priority (SP) services queues based on priority only. As traffic comes into the Switch, traffic on the highest priority queue, Q7 is transmitted first. When that queue empties, traffic on the next highest-priority queue, Q6 is transmitted until Q6 empties, and then traffic is transmitted on Q5 and so on. If higher priority queues never empty, then traffic on lower priority queues never gets sent. SP does not automatically adapt to changing network requirements.

20.1.2 Weighted Fair Queuing

Weighted Fair Queuing is used to guarantee each queue's minimum bandwidth based on its bandwidth weight (the number you configure in the **Weight** field) when there is traffic congestion. WFQ is activated only when a port has more traffic than it can handle. Queues with larger weights get more guaranteed bandwidth than queues with smaller weights. By default, the weight for Q0 is 1, for Q1 is 2, for Q2 is 3, and so on.

The weights range from 1 to 15 and the actual guaranteed bandwidth is calculated as follows:

$2^{(\textbf{Weight} - 1)}$ x 10 KB

If the weight setting is 5, the actual quantum guaranteed to the associated queue would be as follows:

2^4 x 10KB = 320 KB

20.1.3 Weighted Round Robin Scheduling (WRR)

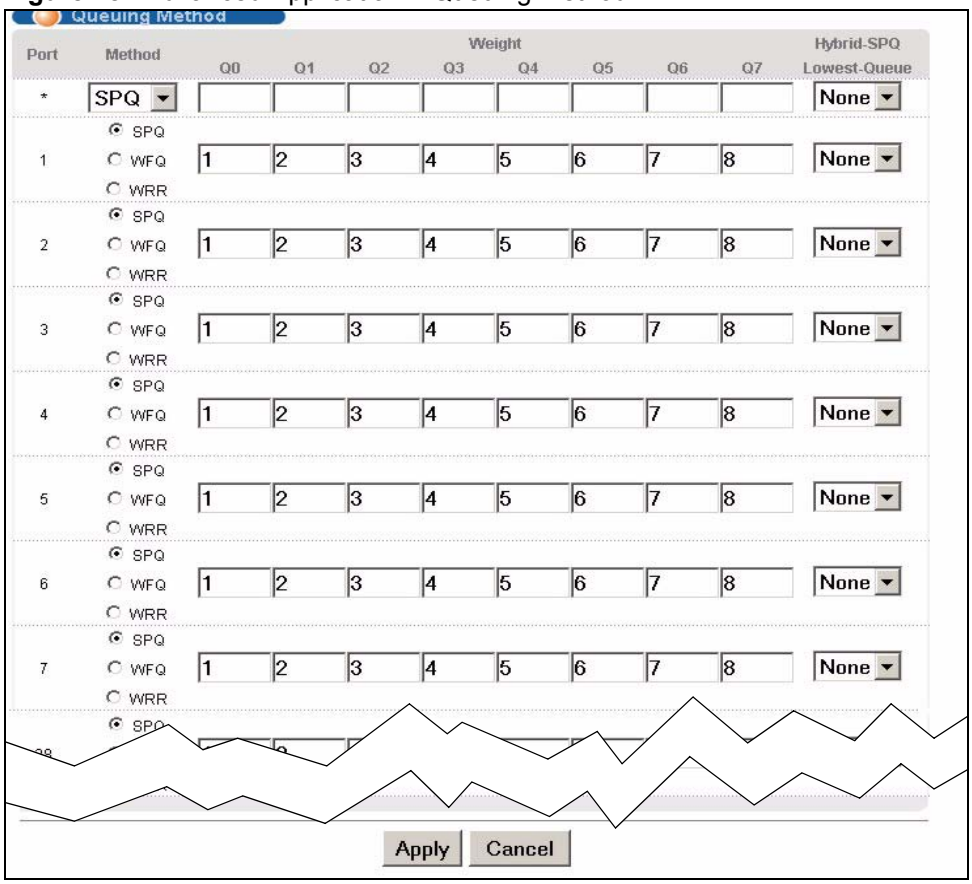
Round Robin Scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

Weighted Round Robin Scheduling (WRR) uses the same algorithm as round robin scheduling, but services queues based on their priority and queue weight (the number you configure in the queue **Weight** field) rather than a fixed amount of bandwidth. WRR is activated only when a port has more traffic than it can handle. Queues with larger weights get more service than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues and returns to queues that have not yet emptied.

20.2 Configuring Queuing

Click **Advanced Application** > **Queuing Method** in the navigation panel.

Figure 78 Advanced Application > Queuing Method



The following table describes the labels in this screen.

Table 50 Advanced Application > Queuing Method

LABEL	DESCRIPTION
Port	This label shows the port you are configuring.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Method	Select **SPQ (Strictly Priority Queuing), WFQ (Weighted Fair Queuing) or WRR (Weighted Round Robin)**. Strictly Priority services queues based on priority only. When the highest priority queue empties, traffic on the next highest-priority queue begins. Q7 has the highest priority and Q0 the lowest. Weighted Fair Queuing is used to guarantee each queue's minimum bandwidth based on their bandwidth weight (the number you configure in the **Weight** field). Queues with larger weights get more guaranteed bandwidth than queues with smaller weights. Weighted Round Robin Scheduling services queues on a rotating basis based on their queue weight (the number you configure in the queue **Weight** field). Queues with larger weights get more service than queues with smaller weights.
Weight	When you select **WFQ** or **WRR** enter the queue weight here. Bandwidth is divided across the different traffic queues according to their weights.
Q0-Q7	This field is applicable only when you select **WFQ** or **WRR**. Select a queue (**Q0** to **Q7**) to have the Switch use **Strictly Priority** to service the subsequent queue(s) after and including the specified queue for the 1000Base-T, 1000Base-X and 10 Gigabit Ethernet ports. For example, if you select **Q5**, the Switch services traffic on **Q5**, **Q6** and **Q7** using **Strictly Priority**. Select **None** to always use **WFQ** or **WRR**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

21

VLAN Stacking

This chapter shows you how to configure VLAN stacking on your Switch. See the chapter on VLANs for more background information on Virtual LAN

21.1 VLAN Stacking Overview

A service provider can use VLAN stacking to allow it to distinguish multiple customers VLANs, even those with the same (customer-assigned) VLAN ID, within its network.

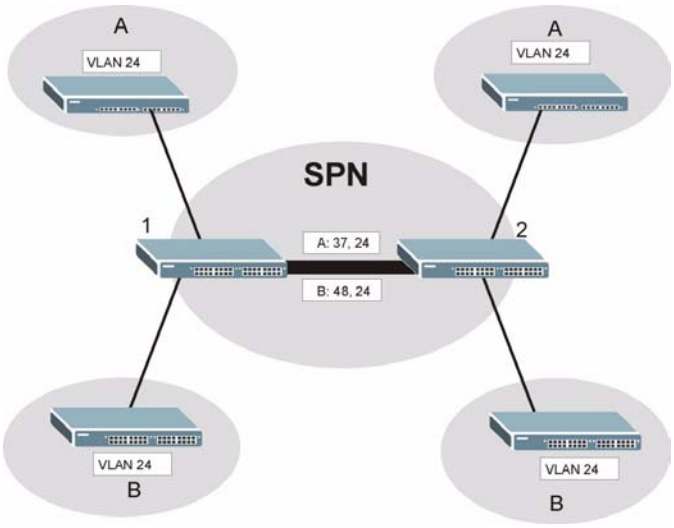
Use VLAN stacking to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter the network. By tagging the tagged frames ("double-tagged" frames), the service provider can manage up to 4,094 VLAN groups with each group containing up to 4,094 customer VLANs. This allows a service provider to provide different service, based on specific VLANs, for many different customers.

A service provider's customers may require a range of VLANs to handle multiple applications. A service provider's customers can assign their own inner VLAN tags on ports for these applications. The service provider can assign an outer VLAN tag for each customer. Therefore, there is no VLAN tag overlap among customers, so traffic from different customers is kept separate.

21.1.1 VLAN Stacking Example

In the following example figure, both **A** and **B** are Service Provider's Network (SPN) customers with VPN tunnels between their head offices and branch offices respectively. Both have an identical VLAN tag for their VLAN group. The service provider can separate these two VLANs within its network by adding tag 37 to distinguish customer **A** and tag 48 to distinguish customer **B** at edge device **1** and then stripping those tags at edge device **2** as the data frames leave the network.

Figure 79 VLAN Stacking Example



21.2 VLAN Stacking Port Roles

Each port can have three VLAN stacking “roles”, **Normal**, **Access Port** and **Tunnel** (the latter is for Gigabit ports only).

- Select **Normal** for “regular” (non-VLAN stacking) IEEE 802.1Q frame switching.
- Select **Access Port** for ingress ports on the service provider's edge devices (**1** and **2** in the VLAN stacking example figure). The incoming frame is treated as "untagged", so a second VLAN tag (outer VLAN tag) can be added.

Static VLAN **Tx Tagging** MUST be disabled on a port where you choose **Normal** or **Access Port**.

- Select **Tunnel Port** (available for Gigabit ports only) for egress ports at the edge of the service provider's network. All VLANs belonging to a customer can be aggregated into a single service provider's VLAN (using the outer VLAN tag defined by the Service Provider’s (SP) VLAN ID (VID)).

Static VLAN **Tx Tagging** MUST be enabled on a port where you choose **Tunnel Port**.

21.3 VLAN Tag Format

A VLAN tag (service provider VLAN stacking or customer IEEE 802.1Q) consists of the following three fields.

Table 51 VLAN Tag Format

Type	Priority	VID

Type is a standard Ethernet type code identifying the frame and indicates that whether the frame carries IEEE 802.1Q tag information. **SP TPID** (Service Provider Tag Protocol Identifier) is the service provider VLAN stacking tag type. Many vendors use 0x8100 or 0x9100.

TPID (Tag Protocol Identifier) is the customer IEEE 802.1Q tag.

- If the VLAN stacking port role is **Access Port**, then the Switch adds the **SP TPID** tag to all incoming frames on the service provider's edge devices (1 and 2 in the VLAN stacking example figure).
- If the VLAN stacking port role is **Tunnel Port**, then the Switch only adds the **SP TPID** tag to all incoming frames on the service provider's edge devices (1 and 2 in the VLAN stacking example figure) that have an **SP TPID** different to the one configured on the Switch. (If an incoming frame's **SP TPID** is the same as the one configured on the Switch, then the Switch will not add the tag.)

Priority refers to the IEEE 802.1p standard that allows the service provider to prioritize traffic based on the class of service (CoS) the customer has paid for.

- On the Switch, configure priority level of the inner IEEE 802.1Q tag in the **Port Setup** screen.
- "0" is the lowest priority level and "7" is the highest.

VID is the VLAN ID. **SP VID** is the VID for the second (service provider's) VLAN tag.

21.3.1 Frame Format

The frame format for an untagged Ethernet frame, a single-tagged 802.1Q frame (customer) and a "double-tagged" 802.1Q frame (service provider) is shown next.

Configure the fields as highlighted in the Switch **VLAN Stacking** screen.

Table 52 Single and Double Tagged 802.11Q Frame Format

						DA	SA	Len/ Etype	Data	FCS	Untagged Ethernet frame
			DA	SA	**TPID**	**Priority**	**VID**	Len/ Etype	Data	FCS	IEEE 802.1Q customer tagged frame
DA	SA	**SPTPID**	**Priority**	**VID**	**TPID**	**Priority**	**VID**	Len/ Etype	Data	FCS	Double-tagged frame

Table 53 802.1Q Frame

DA	Destination Address	Priority	802.1p Priority
SA	Source Address	Len/ Etype	Length and type of Ethernet frame

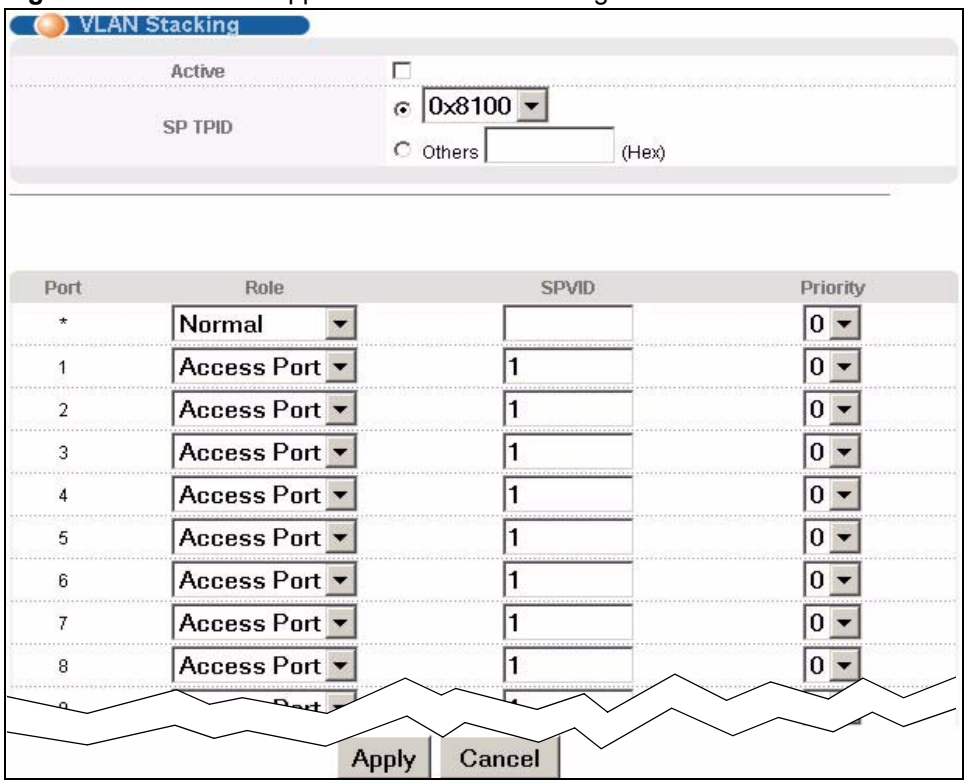
Table 53 802.1Q Frame

(SP)TPID	(Service Provider) Tag Protocol IDentifier	Data	Frame data
VID	VLAN ID	FCS	Frame Check Sequence

21.4 Configuring VLAN Stacking

Click **Advanced Applications > VLAN Stacking** to display the screen as shown.

Figure 80 Advanced Application > VLAN Stacking



The following table describes the labels in this screen.

Table 54 Advanced Application > VLAN Stacking

LABEL	DESCRIPTION
Active	Select this checkbox to enable VLAN stacking on the Switch.
SP TPID	**SP TPID** is a standard Ethernet type code identifying the frame and indicates whether the frame carries IEEE 802.1Q tag information. Choose **0x8100** or **0x9100** from the drop-down list box or select **Others** and then enter a four-digit hexadecimal number from 0x0000 to 0xFFFF. 0x denotes a hexadecimal number. It does not have to be typed in the **Others** text field.
Port	The port number identifies the port you are configuring.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.

Table 54 Advanced Application > VLAN Stacking (continued)

LABEL	DESCRIPTION
Role	Select **Normal** to have the Switch ignore frames received (or transmitted) on this port with VLAN stacking tags. Anything you configure in **SPVID** and **Priority** are ignored. Select **Access Port** to have the Switch add the **SP TPID** tag to all incoming frames received on this port. Select **Access Port** for ingress ports at the edge of the service provider's network. Select **Tunnel Port** (available for Gigabit ports only) for egress ports at the edge of the service provider's network. In order to support VLAN stacking on a port, the port must be able to allow frames of 1526 Bytes (1522 Bytes + 4 Bytes for the second tag) to pass through it.
SPVID	**SPVID** is the service provider's VLAN ID (the outer VLAN tag). Enter the service provider ID (from 1 to 4094) for frames received on this port. See Chapter 8 on page 87 for more background information on VLAN ID.
Priority	On the Switch, configure priority level of inner IEEE 802.1Q tag in the **Port Setup** screen. "0" is the lowest priority level and "7" is the highest.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

22

Multicast

This chapter shows you how to configure various multicast features.

22.1 Multicast Overview

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender to 1 recipient) or Broadcast (1 sender to everybody on the network). Multicast delivers IP packets to just a group of hosts on the network.

IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data. Refer to RFC 1112, RFC 2236 and RFC 3376 for information on IGMP versions 1, 2 and 3 respectively.

22.1.1 IP Multicast Addresses

In IPv4, a multicast address allows a device to send packets to a specific group of hosts (multicast group) in a different subnetwork. A multicast IP address represents a traffic receiving group, not individual receiving devices. IP addresses in the Class D range (224.0.0.0 to 239.255.255.255) are used for IP multicasting. Certain IP multicast numbers are reserved by IANA for special purposes (see the IANA website for more information).

22.1.2 IGMP Filtering

With the IGMP filtering feature, you can control which IGMP groups a subscriber on a port can join. This allows you to control the distribution of multicast services (such as content information distribution) based on service plans and types of subscription.

You can set the Switch to filter the multicast group join reports on a per-port basis by configuring an IGMP filtering profile and associating the profile to a port.

22.1.3 IGMP Snooping

The Switch can passively snoop on IGMP packets transferred between IP multicast routers/ switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the Switch to learn multicast groups without you having to manually configure them.

The Switch forwards multicast traffic destined for multicast groups (that it has learned from IGMP snooping or that you have manually configured) to ports that are members of that group. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your Switch.

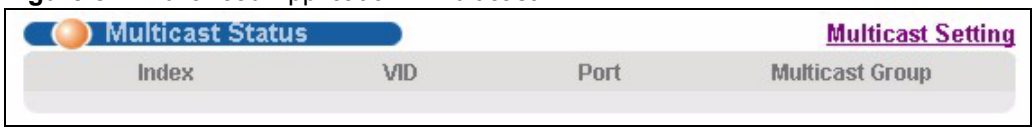
22.1.4 IGMP Snooping and VLANs

The Switch can perform IGMP snooping on up to 16 VLANs. You can configure the Switch to automatically learn multicast group membership of any VLANs. The Switch then performs IGMP snooping on the first 16 VLANs that send IGMP packets. This is referred to as auto mode. Alternatively, you can specify the VLANs that IGMP snooping should be performed on. This is referred to as fixed mode. In fixed mode the Switch does not learn multicast group membership of any VLANs other than those explicitly added as an IGMP snooping VLAN.

22.2 Multicast Status

Click **Advanced Applications > Multicast** to display the screen as shown. This screen shows the multicast group information. See Section 22.1 on page 173 for more information on multicasting.

Figure 81 Advanced Application > Multicast



The following table describes the labels in this screen.

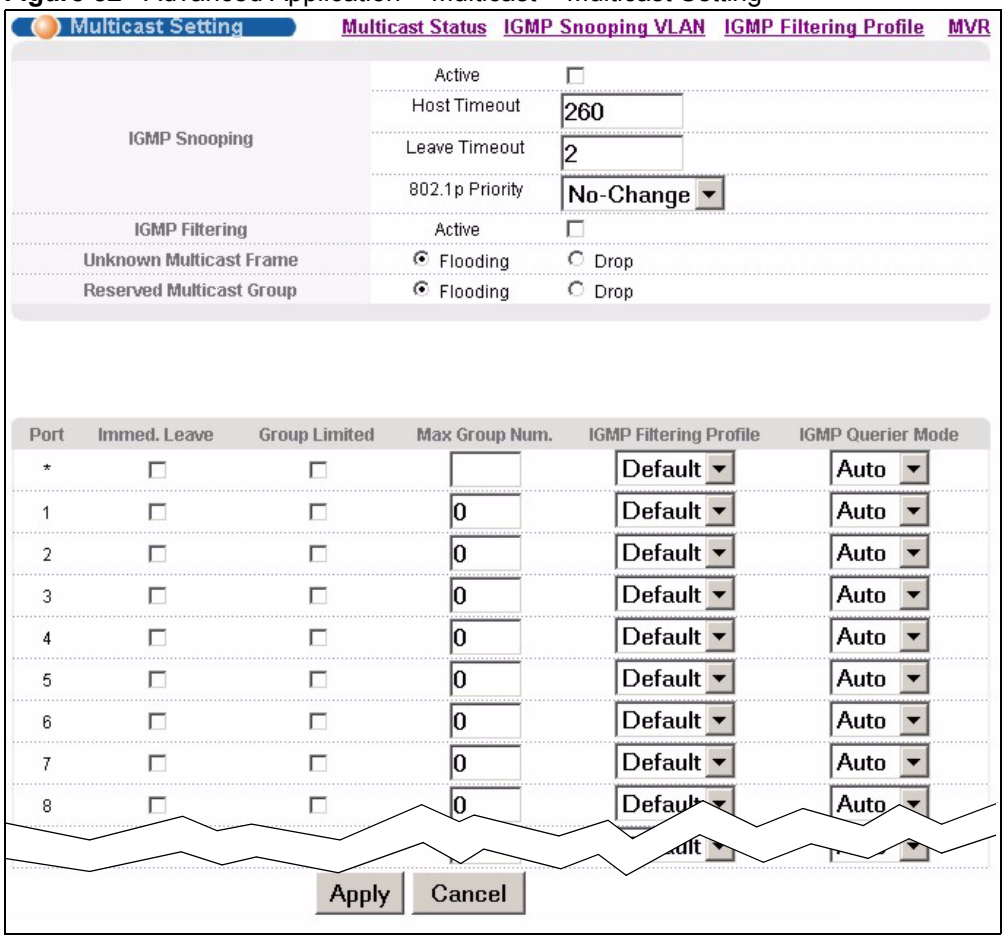
Table 55 Multicast Status

LABEL	DESCRIPTION
Index	This is the index number of the entry.
VID	This field displays the multicast VLAN ID.
Port	This field displays the port number that belongs to the multicast group.
Multicast Group	This field displays IP multicast group addresses.

22.3 Multicast Setting

Click **Advanced Applications > Multicast > Multicast Setting** link to display the screen as shown. See Section 22.1 on page 173 for more information on multicasting.

Figure 82 Advanced Application > Multicast > Multicast Setting



The following table describes the labels in this screen.

Table 56 Advanced Application > Multicast > Multicast Setting

LABEL	DESCRIPTION
IGMP Snooping	Use these settings to configure IGMP Snooping.
Active	Select **Active** to enable IGMP Snooping to forward group multicast traffic only to ports that are members of that group.
Host Timeout	Specify the time (from 1 to 16 711 450) in seconds that elapses before the Switch removes an IGMP group membership entry if it does not receive report messages from the port.
Leave Timeout	Enter an IGMP leave timeout value (from 1 to 16 711 450) in seconds. This defines how many seconds the Switch waits for an IGMP report before removing an IGMP snooping membership entry when an IGMP leave message is received from a host.
802.1p Priority	Select a priority level (0-7) to which the Switch changes the priority in outgoing IGMP control packets. Otherwise, select **No-Change** to not replace the priority.
IGMP Filtering	Select **Active** to enable IGMP filtering to control which IGMP groups a subscriber on a port can join. Note: If you enable IGMP filtering, you must create and assign IGMP filtering profiles for the ports that you want to allow to join multicast groups.

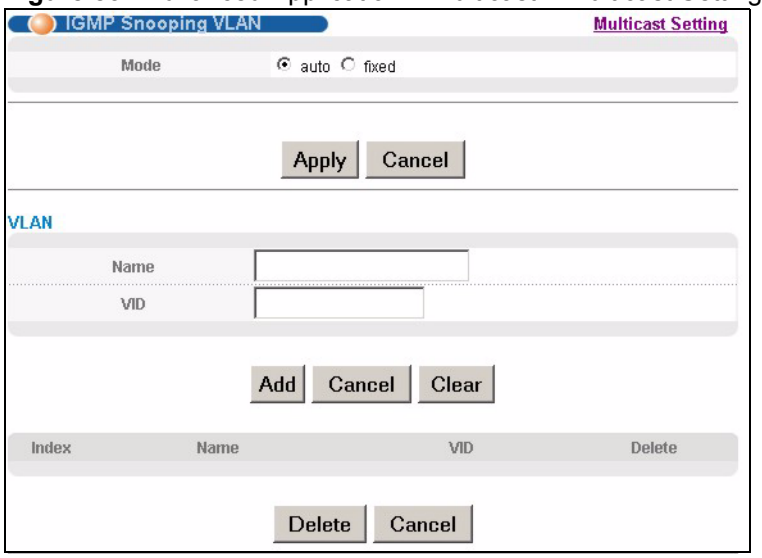
Table 56 Advanced Application > Multicast > Multicast Setting (continued)

LABEL	DESCRIPTION
Unknown Multicast Frame	Specify the action to perform when the Switch receives an unknown multicast frame. Select **Drop** to discard the frame(s). Select **Flooding** to send the frame(s) to all ports.
Reserved Multicast Group	Multicast addresses (224.0.0.0 to 224.0.0.255) are reserved for the local scope. For examples, 224.0.0.1 is for all hosts in this subnet, 224.0.0.2 is for all multicast routers in this subnet, etc. A router will not forward a packet with the destination IP address within this range. See the IANA website for more information. Specify the action to perform when the Switch receives a frame with a reserved multicast address. Select **Drop** to discard the frame(s). Select **Flooding** to send the frame(s) to all ports.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Immed. Leave	Select this option to set the Switch to remove this port from the multicast tree when an IGMP version 2 leave message is received on this port. Select this option if there is only one host connected to this port.
Group Limited	Select this option to limit the number of multicast groups this port is allowed to join.
Max Group Num.	Enter the number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report frame(s) is dropped on this port.
IGMP Filtering Profile	Select the name of the IGMP filtering profile to use for this port. Otherwise, select **Default** to prohibit the port from joining any multicast group. You can create IGMP filtering profiles in the **Multicast** > **Multicast Setting** > **IGMP Filtering Profile** screen.
IGMP Querier Mode	The Switch treats an IGMP query port as being connected to an IGMP multicast router (or server). The Switch forwards IGMP join or leave packets to an IGMP query port. Select **Auto** to have the Switch use the port as an IGMP query port if the port receives IGMP query packets. Select **Fixed** to have the Switch always use the port as an IGMP query port. Select this when you connect an IGMP multicast server to the port. Select **Edge** to stop the Switch from using the port as an IGMP query port. The Switch will not keep any record of an IGMP router being connected to this port. The Switch does not forward IGMP join or leave packets to this port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

22.4 IGMP Snooping VLAN

Click **Advanced Applications > Multicast** in the navigation panel. Click the **Multicast Setting** link and then the **IGMP Snooping VLAN** link to display the screen as shown. See Section 22.1.4 on page 174 for more information on IGMP Snooping VLAN.

Figure 83 Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN



The following table describes the labels in this screen.

Table 57 Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN

LABEL	DESCRIPTION
Mode	Select **auto** to have the Switch learn multicast group membership information of any VLANs automatically. Select **fixed** to have the Switch only learn multicast group membership information of the VLAN(s) that you specify below. In either **auto** or **fixed** mode, the Switch can learn up to 16 VLANs (including up to three VLANs you configured in the **MVR** screen). For example, if you have configured one multicast VLAN in the **MVR** screen, you can only specify up to 15 VLANs in this screen. The Switch drops any IGMP control messages which do not belong to these 16 VLANs. Note: You must also enable IGMP snooping in the **Multicast Setting** screen first.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
VLAN	Use this section of the screen to add VLANs upon which the Switch is to perform IGMP snooping.
Name	Enter the descriptive name of the VLAN for identification purposes.

Table 57 Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN

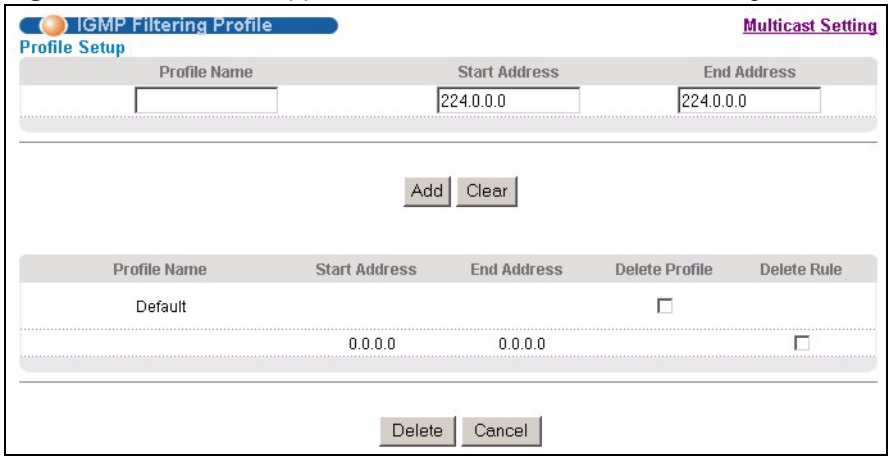
LABEL	DESCRIPTION
VID	Enter the ID of a static VLAN; the valid range is between 1 and 4094. Note: You cannot configure the same VLAN ID as in the **MVR** screen.
Add	Click **Add** to insert the entry in the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click this to clear the fields.
Index	This is the number of the IGMP snooping VLAN entry in the table.
Name	This field displays the descriptive name for this VLAN group.
VID	This field displays the ID number of the VLAN group.
Delete	Check the rule(s) that you want to remove in the **Delete** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

22.5 IGMP Filtering Profile

An IGMP filtering profile specifies a range of multicast groups that clients connected to the Switch are able to join. A profile contains a range of multicast IP addresses which you want clients to be able to join. Profiles are assigned to ports (in the **Multicast Setting** screen). Clients connected to those ports are then able to join the multicast groups specified in the profile. Each port can be assigned a single profile. A profile can be assigned to multiple ports.

Click **Advanced Applications** > **Multicast** > **Multicast Setting** > **IGMP Filtering Profile** link to display the screen as shown.

Figure 84 Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile



The following table describes the labels in this screen.

Table 58 Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile for identification purposes. To configure additional rule(s) for a profile that you have already added, enter the profile name and specify a different IP multicast address range.
Start Address	Type the starting multicast IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile.
End Address	Type the ending multicast IP address for a range of IP addresses that you want to belong to the IGMP filter profile. If you want to add a single multicast IP address, enter it in both the **Start Address** and **End Address** fields.
Add	Click **Add** to save the profile to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click **Clear** to clear the fields to the factory defaults.
Profile Name	This field displays the descriptive name of the profile.
Start Address	This field displays the start of the multicast address range.
End Address	This field displays the end of the multicast address range.
Delete	To delete the profile(s) and all the accompanying rules, select the profile(s) that you want to remove in the **Delete Profile** column, then click the **Delete** button. To delete a rule(s) from a profile, select the rule(s) that you want to remove in the **Delete Rule** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete Profile**/**Delete Rule** check boxes.

22.6 MVR Overview

Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) that use multicast traffic across an Ethernet ring-based service provider network.

MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network. While isolated in different subscriber VLANs, connected devices can subscribe to and unsubscribe from the multicast stream in the multicast VLAN. This improves bandwidth utilization with reduced multicast traffic in the subscriber VLANs and simplifies multicast group management.

MVR only responds to IGMP join and leave control messages from multicast groups that are configured under MVR. Join and leave reports from other multicast groups are managed by IGMP snooping.

The following figure shows a network example. The subscriber VLAN (**1**, **2** and **3**) information is hidden from the streaming media server, **S**. In addition, the multicast VLAN information is only visible to the Switch and **S**.

Figure 85 MVR Network Example

22.6.1 Types of MVR Ports

In MVR, a source port is a port on the Switch that can send and receive multicast traffic in a multicast VLAN while a receiver port can only receive multicast traffic. Once configured, the Switch maintains a forwarding table that matches the multicast stream to the associated multicast group.

22.6.2 MVR Modes

You can set your Switch to operate in either dynamic or compatible mode.

In dynamic mode, the Switch sends IGMP leave and join reports to the other multicast devices (such as multicast routers or servers) in the multicast VLAN. This allows the multicast devices to update the multicast forwarding table to forward or not forward multicast traffic to the receiver ports.

In compatible mode, the Switch does not send any IGMP reports. In this case, you must manually configure the forwarding settings on the multicast devices in the multicast VLAN.

22.6.3 How MVR Works

The following figure shows a multicast television example where a subscriber device (such as a computer) in VLAN 1 receives multicast traffic from the streaming media server, **S**, via the Switch. Multiple subscriber devices can connect through a port configured as the receiver on the Switch.

When the subscriber selects a television channel, computer **A** sends an IGMP report to the Switch to join the appropriate multicast group. If the IGMP report matches one of the configured MVR multicast group addresses on the Switch, an entry is created in the forwarding table on the Switch. This maps the subscriber VLAN to the list of forwarding destinations for the specified multicast traffic.

When the subscriber changes the channel or turns off the computer, an IGMP leave message is sent to the Switch to leave the multicast group. The Switch sends a query to VLAN 1 on the receiver port (in this case, an uplink port on the Switch). If there is another subscriber device connected to this port in the same subscriber VLAN, the receiving port will still be on the list of forwarding destination for the multicast traffic. Otherwise, the Switch removes the receiver port from the forwarding table.

Figure 86 MVR Multicast Television Example

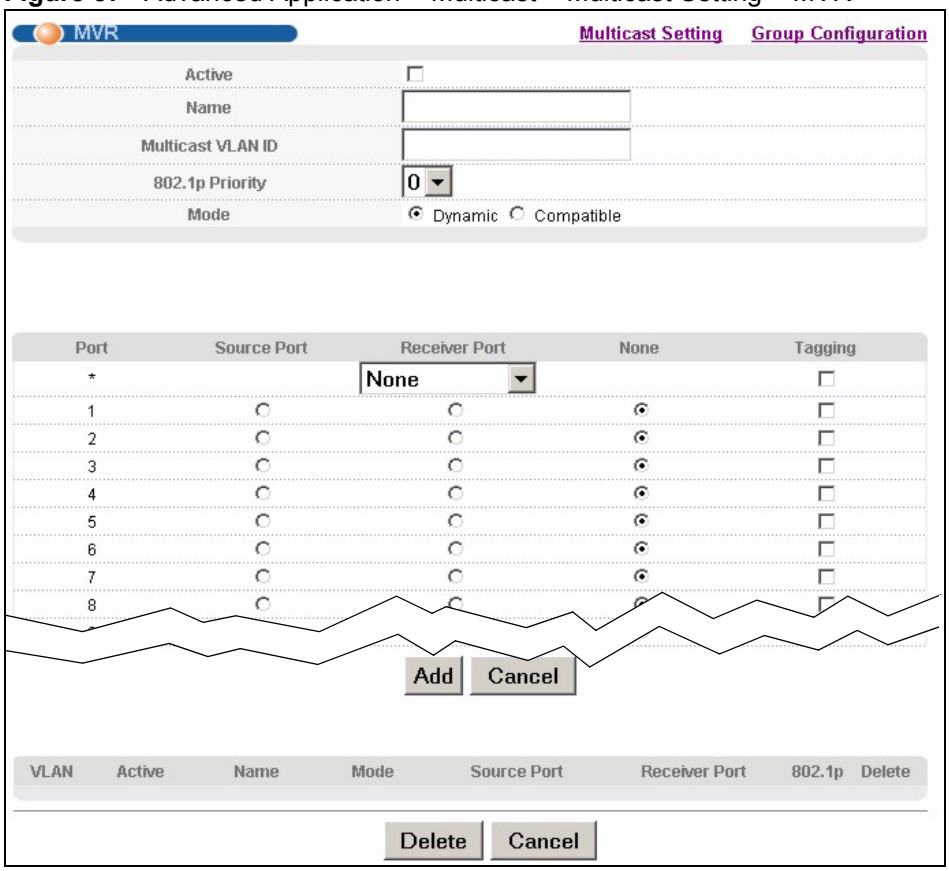
22.7 General MVR Configuration

Use the **MVR** screen to create multicast VLANs and select the receiver port(s) and a source port for each multicast VLAN. Click **Advanced Applications > Multicast** > **Multicast Setting > MVR** link to display the screen as shown next.

You can create up to three multicast VLANs and up to 256 multicast rules on the Switch.

Your Switch automatically creates a static VLAN (with the same VID) when you create a multicast VLAN in this screen.

Figure 87 Advanced Application > Multicast > Multicast Setting > MVR



The following table describes the related labels in this screen.

Table 59 Advanced Application > Multicast > Multicast Setting > MVR

LABEL	DESCRIPTION
Active	Select this check box to enable MVR to allow one single multicast VLAN to be shared among different subscriber VLANs on the network.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Multicast VLAN ID	Enter the VLAN ID (1 to 4094) of the multicast VLAN.
802.1p Priority	Select a priority level (0-7) with which the Switch replaces the priority in outgoing IGMP control packets (belonging to this multicast VLAN).
Mode	Specify the MVR mode on the Switch. Choices are **Dynamic** and **Compatible**. Select **Dynamic** to send IGMP reports to all MVR source ports in the multicast VLAN. Select **Compatible** to set the Switch not to send IGMP reports.
Port	This field displays the port number on the Switch.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.

Table 59 Advanced Application > Multicast > Multicast Setting > MVR (continued)

LABEL	DESCRIPTION
Source Port	Select this option to set this port as the MVR source port that sends and receives multicast traffic. All source ports must belong to a single multicast VLAN.
Receiver Port	Select this option to set this port as a receiver port that only receives multicast traffic.
None	Select this option to set the port not to participate in MVR. No MVR multicast traffic is sent or received on this port.
Tagging	Select this checkbox if you want the port to tag the VLAN ID in all outgoing frames transmitted.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
VLAN	This field displays the multicast VLAN ID.
Active	This field displays whether the multicast group is enabled or not.
Name	This field displays the descriptive name for this setting.
Mode	This field displays the MVR mode.
Source Port	This field displays the source port number(s).
Receiver Port	This field displays the receiver port number(s).
802.1p	This field displays the priority level.
Delete	To delete a multicast VLAN(s), select the rule(s) that you want to remove in the **Delete** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

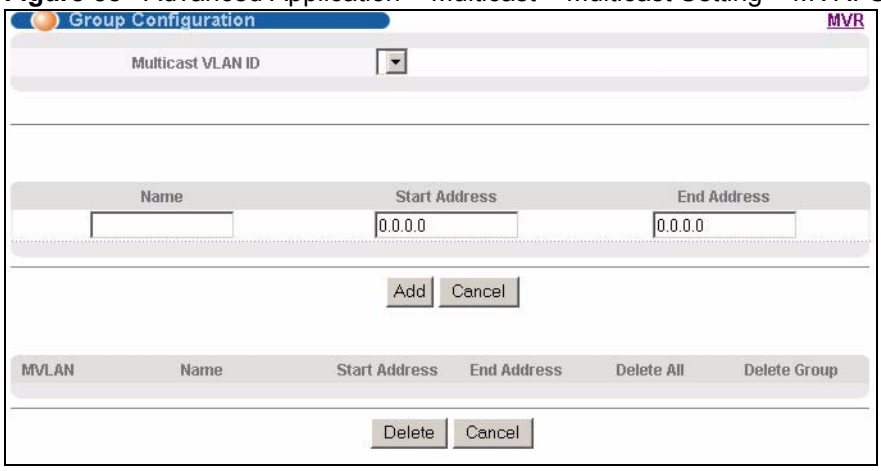
22.8 MVR Group Configuration

All source ports and receiver ports belonging to a multicast group can receive multicast data sent to this multicast group.

Configure MVR IP multicast group address(es) in the **Group Configuration** screen. Click **Group Configuration** in the **MVR** screen.

A port can belong to more than one multicast VLAN. However, IP multicast group addresses in different multicast VLANs cannot overlap.

Figure 88 Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration



The following table describes the labels in this screen.

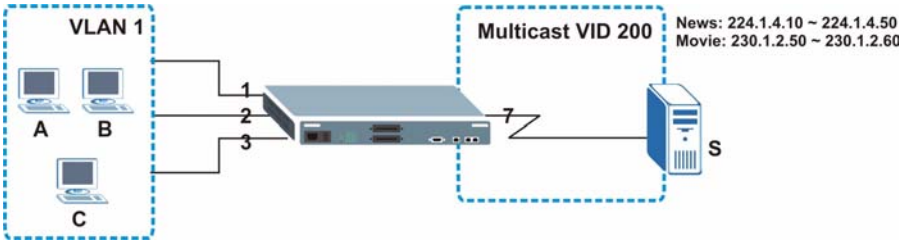
Table 60 Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration

LABEL	DESCRIPTION
Multicast VLAN ID	Select a multicast VLAN ID (that you configured in the **MVR** screen) from the drop-down list box.
Name	Enter a descriptive name for identification purposes.
Start Address	Enter the starting IP multicast address of the multicast group in dotted decimal notation. Refer to Section 22.1.1 on page 173 for more information on IP multicast addresses.
End Address	Enter the ending IP multicast address of the multicast group in dotted decimal notation. Enter the same IP address as the **Start Address** field if you want to configure only one IP address for a multicast group. Refer to Section 22.1.1 on page 173 for more information on IP multicast addresses.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
MVLAN	This field displays the multicast VLAN ID.
Name	This field displays the descriptive name for this setting.
Start Address	This field displays the starting IP address of the multicast group.
End Address	This field displays the ending IP address of the multicast group.
Delete	Select **Delete All** or **Delete Group** and click **Delete** to remove the selected entry(ies) from the table.
Cancel	Select **Cancel** to clear the checkbox(es) in the table.

22.8.1 MVR Configuration Example

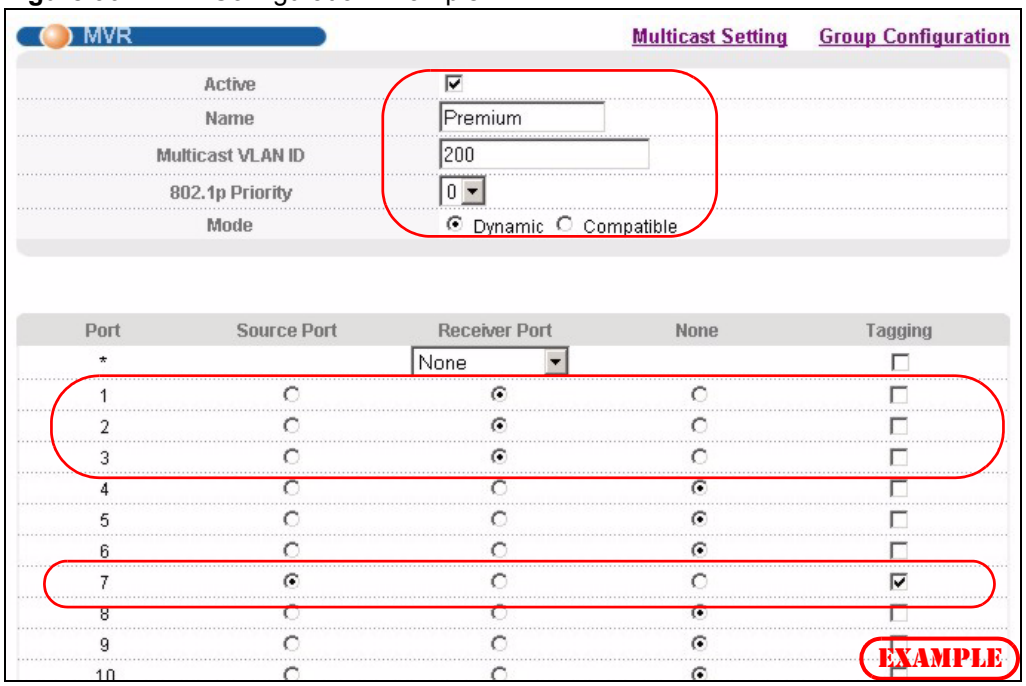
The following figure shows a network example where ports 1, 2 and 3 on the Switch belong to VLAN 1. In addition, port 7 belongs to the multicast group with VID 200 to receive multicast traffic (the **News** and **Movie** channels) from the remote streaming media server, **S**. Computers A, B and C in VLAN 1 are able to receive the traffic.

Figure 89 MVR Configuration Example



To configure the MVR settings on the Switch, create a multicast group in the **MVR** screen and set the receiver and source ports.

Figure 90 MVR Configuration Example



To set the Switch to forward the multicast group traffic to the subscribers, configure multicast group settings in the **Group Configuration** screen. The following figure shows an example where two multicast groups (**News** and **Movie**) are configured for the multicast VLAN 200.

Figure 91 MVR Group Configuration Example

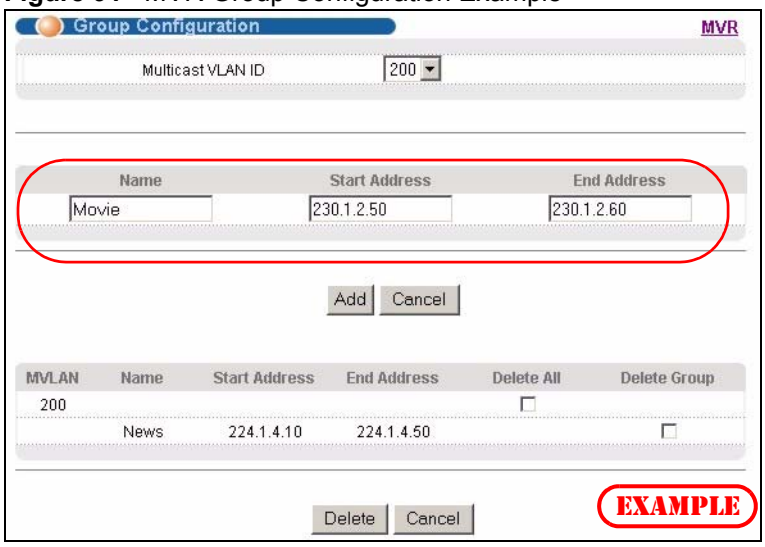
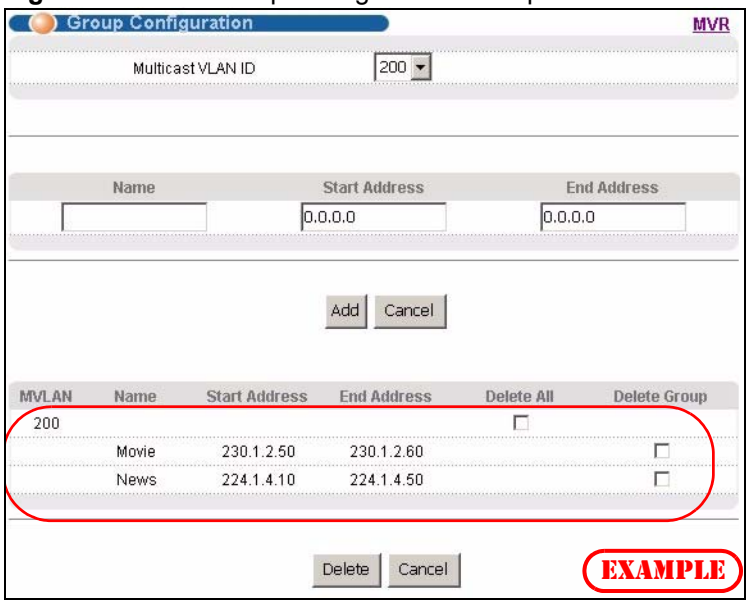


Figure 92 MVR Group Configuration Example



23

Authentication & Accounting

This chapter describes how to configure authentication and accounting settings on the Switch.

23.1 Authentication, Authorization and Accounting

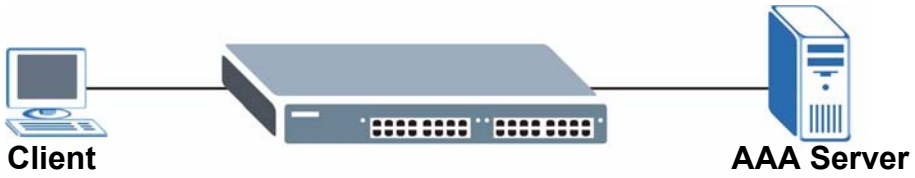
Authentication is the process of determining who a user is and validating access to the Switch. The Switch can authenticate users who try to log in based on user accounts configured on the Switch itself. The Switch can also use an external authentication server to authenticate a large number of users.

Authorization is the process of determining what a user is allowed to do. Different user accounts may have higher or lower privilege levels associated with them. For example, user A may have the right to create new login accounts on the Switch but user B cannot. The Switch can authorize users based on user accounts configured on the Switch itself or it can use an external server to authorize a large number of users.

Accounting is the process of recording what a user is doing. The Switch can use an external server to track when users log in, log out, execute commands and so on. Accounting can also record system related actions such as boot up and shut down times of the Switch.

The external servers that perform authentication, authorization and accounting functions are known as AAA servers. The Switch supports RADIUS (Remote Authentication Dial-In User Service, see Section 23.1.2 on page 188) and TACACS+ (Terminal Access Controller Access-Control System Plus, see Section 23.1.2 on page 188) as external authentication, authorization and accounting servers.

Figure 93 AAA Server



23.1.1 Local User Accounts

By storing user profiles locally on the Switch, your Switch is able to authenticate and authorize users without interacting with a network AAA server. However, there is a limit on the number of users you may authenticate in this way (See Chapter 35 on page 285).

23.1.2 RADIUS and TACACS+

RADIUS and TACACS+ are security protocols used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS and TACACS+ authentication both allow you to validate an unlimited number of users from a central location.

The following table describes some key differences between RADIUS and TACACS+.

Table 61 RADIUS vs TACACS+

	RADIUS	TACACS+
Transport Protocol	UDP (User Datagram Protocol)	TCP (Transmission Control Protocol)
Encryption	Encrypts the password sent for authentication.	All communication between the client (the Switch) and the TACACS server is encrypted.

23.2 Authentication and Accounting Screens

To enable authentication, accounting or both on the Switch. First, configure your authentication server settings (RADIUS, TACACS+ or both) and then set up the authentication priority and accounting settings.

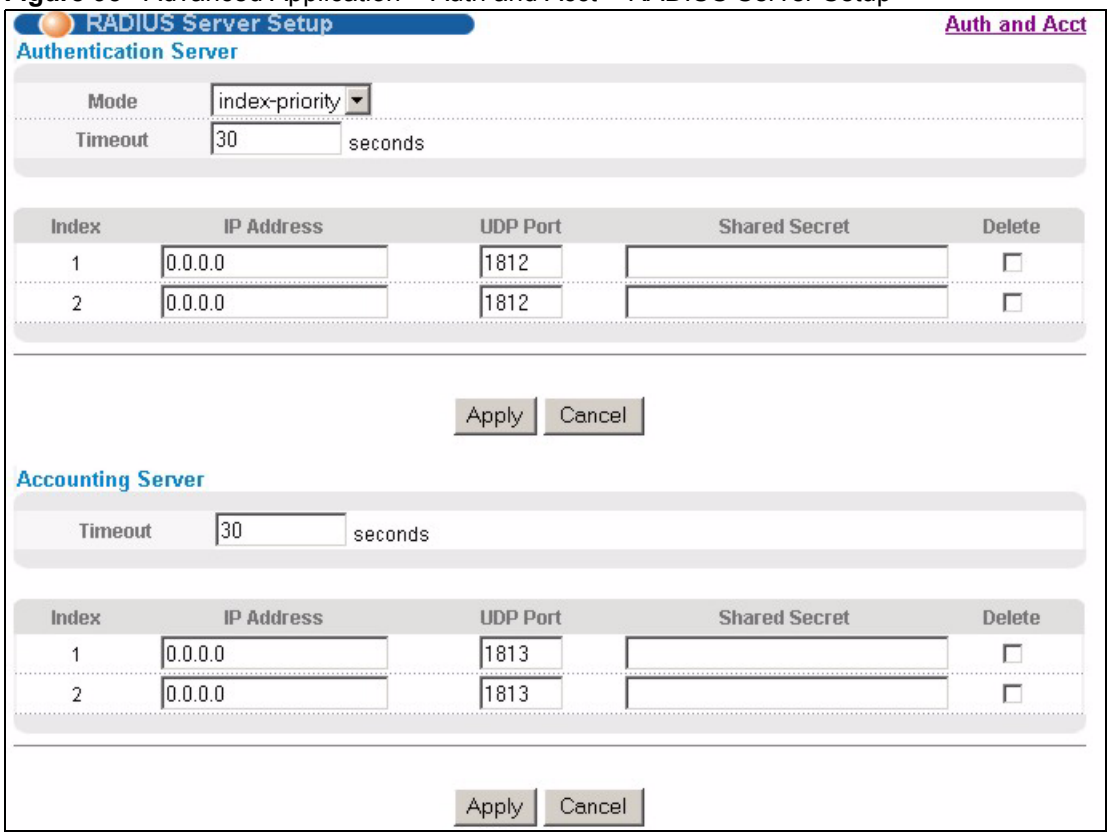
Click **Advanced Application** > **Auth and Acct** in the navigation panel to display the screen as shown.

Figure 94 Advanced Application > Auth and Acct

23.2.1 RADIUS Server Setup

Use this screen to configure your RADIUS server settings. See Section 23.1.2 on page 188 for more information on RADIUS servers. Click on the **RADIUS Server Setup** link in the **Authentication and Accounting** screen to view the screen as shown.

Figure 95 Advanced Application > Auth and Acct > RADIUS Server Setup



The following table describes the labels in this screen.

Table 62 Advanced Application > Auth and Acct > RADIUS Server Setup

LABEL	DESCRIPTION
Authentication Server	Use this section to configure your RADIUS authentication settings.
Mode	This field only applies if you configure multiple RADIUS servers. Select **index-priority** and the Switch tries to authenticate with the first configured RADIUS server, if the RADIUS server does not respond then the Switch tries to authenticate with the second RADIUS server. Select **round-robin** to alternate between the RADIUS servers that it sends authentication requests to.
Timeout	Specify the amount of time in seconds that the Switch waits for an authentication request response from the RADIUS server. If you are using **index-priority** for your authentication and you are using two RADIUS servers then the timeout value is divided between the two RADIUS servers. For example, if you set the timeout value to 30 seconds, then the Switch waits for a response from the first RADIUS server for 15 seconds and then tries the second RADIUS server.
Index	This is a read-only number representing a RADIUS server entry.
IP Address	Enter the IP address of an external RADIUS server in dotted decimal notation.
UDP Port	The default port of a RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the Switch.

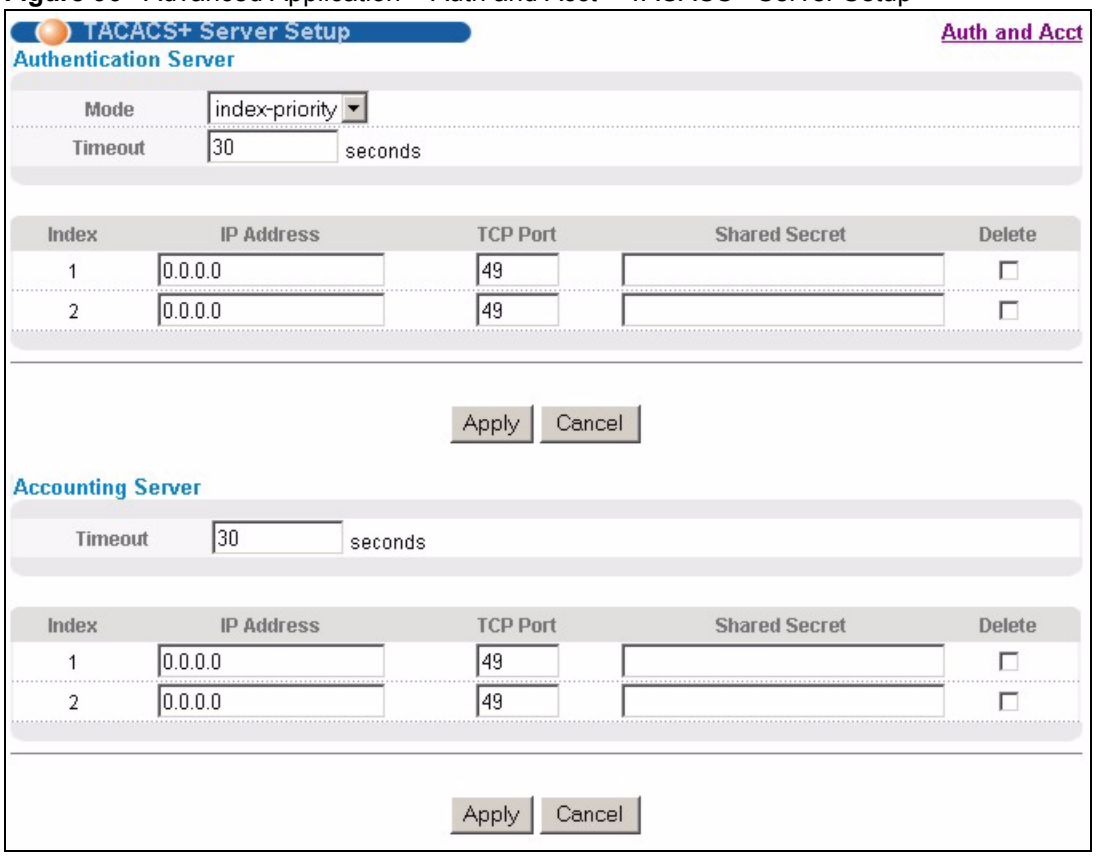
Table 62 Advanced Application > Auth and Acct > RADIUS Server Setup (continued)

LABEL	DESCRIPTION
Delete	Check this box if you want to remove an existing RADIUS server entry from the Switch. This entry is deleted when you click **Apply**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Accounting Server	Use this section to configure your RADIUS accounting server settings.
Timeout	Specify the amount of time in seconds that the Switch waits for an accounting request response from the RADIUS accounting server.
Index	This is a read-only number representing a RADIUS accounting server entry.
IP Address	Enter the IP address of an external RADIUS accounting server in dotted decimal notation.
UDP Port	The default port of a RADIUS accounting server for accounting is **1813**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS accounting server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS accounting server and the Switch.
Delete	Check this box if you want to remove an existing RADIUS accounting server entry from the Switch. This entry is deleted when you click **Apply**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

23.2.2 TACACS+ Server Setup

Use this screen to configure your TACACS+ server settings. See Section 23.1.2 on page 188 for more information on TACACS+ servers. Click on the **TACACS+ Server Setup** link in the **Authentication and Accounting** screen to view the screen as shown.

Figure 96 Advanced Application > Auth and Acct > TACACS+ Server Setup



The following table describes the labels in this screen.

Table 63 Advanced Application > Auth and Acct > TACACS+ Server Setup

LABEL	DESCRIPTION
Authentication Server	Use this section to configure your TACACS+ authentication settings.
Mode	This field is only valid if you configure multiple TACACS+ servers. Select **index-priority** and the Switch tries to authenticate with the first configured TACACS+ server, if the TACACS+ server does not respond then the Switch tries to authenticate with the second TACACS+ server. Select **round-robin** to alternate between the TACACS+ servers that it sends authentication requests to.
Timeout	Specify the amount of time in seconds that the Switch waits for an authentication request response from the TACACS+ server. If you are using **index-priority** for your authentication and you are using two TACACS+ servers then the timeout value is divided between the two TACACS+ servers. For example, if you set the timeout value to 30 seconds, then the Switch waits for a response from the first TACACS+ server for 15 seconds and then tries the second TACACS+ server.
Index	This is a read-only number representing a TACACS+ server entry.
IP Address	Enter the IP address of an external TACACS+ server in dotted decimal notation.
TCP Port	The default port of a TACACS+ server for authentication is **49**. You need not change this value unless your network administrator instructs you to do so.

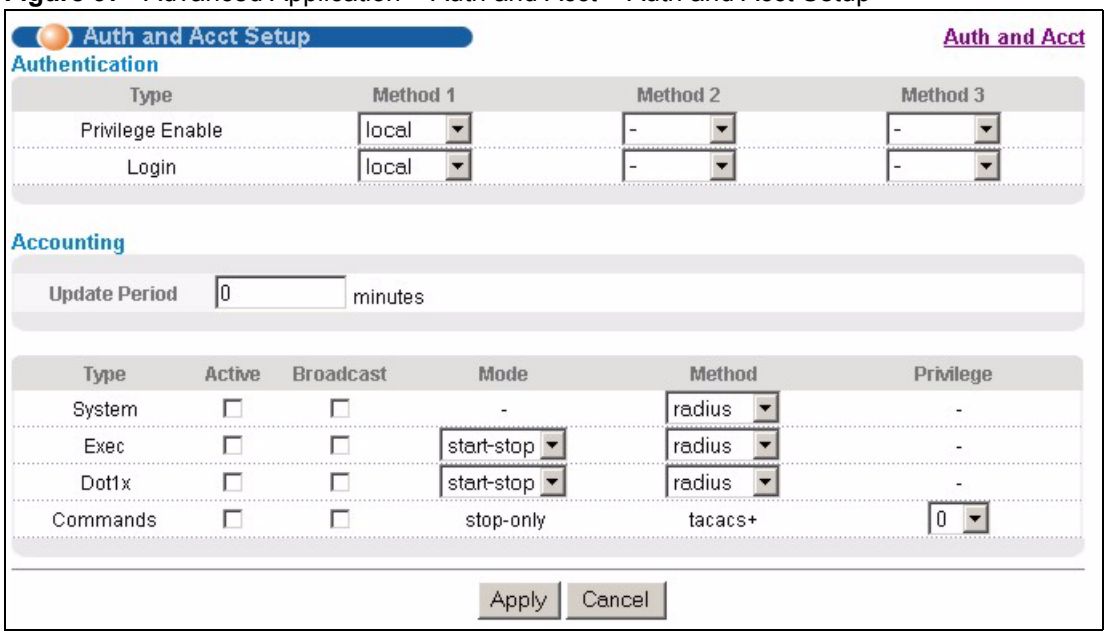
Table 63 Advanced Application > Auth and Acct > TACACS+ Server Setup (continued)

LABEL	DESCRIPTION
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external TACACS+ server and the Switch. This key is not sent over the network. This key must be the same on the external TACACS+ server and the Switch.
Delete	Check this box if you want to remove an existing TACACS+ server entry from the Switch. This entry is deleted when you click **Apply**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Accounting Server	Use this section to configure your TACACS+ accounting settings.
Timeout	Specify the amount of time in seconds that the Switch waits for an accounting request response from the TACACS+ server.
Index	This is a read-only number representing a TACACS+ accounting server entry.
IP Address	Enter the IP address of an external TACACS+ accounting server in dotted decimal notation.
TCP Port	The default port of a TACACS+ accounting server is **49**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external TACACS+ accounting server and the Switch. This key is not sent over the network. This key must be the same on the external TACACS+ accounting server and the Switch.
Delete	Check this box if you want to remove an existing TACACS+ accounting server entry from the Switch. This entry is deleted when you click **Apply**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

23.2.3 Authentication and Accounting Setup

Use this screen to configure authentication and accounting settings on the Switch. Click on the **Auth and Acct Setup** link in the **Authentication and Accounting** screen to view the screen as shown.

Figure 97 Advanced Application > Auth and Acct > Auth and Acct Setup



The following table describes the labels in this screen.

Table 64 Advanced Application > Auth and Acct > Auth and Acct Setup

LABEL	DESCRIPTION
Authentication	Use this section to specify the methods used to authenticate users accessing the Switch.
Privilege Enable	These fields specify which database the Switch should use (first, second and third) to authenticate access privilege level for administrator accounts (users for Switch management). Configure the access privilege of accounts via commands (See Section 44.7 on page 336) for **local** authentication. The **TACACS+** and **RADIUS** are external servers. Before you specify the priority, make sure you have set up the corresponding database correctly first. You can specify up to three methods for the Switch to authenticate the access privilege level of administrators. The Switch checks the methods in the order you configure them (first **Method 1**, then **Method 2** and finally **Method 3**). You must configure the settings in the **Method 1** field. If you want the Switch to check other sources for access privilege level specify them in **Method 2** and **Method 3** fields. Select **local** to have the Switch check the access privilege configured for local authentication. Select **radius** or **tacacs+** to have the Switch check the access privilege via the external servers.

Table 64 Advanced Application > Auth and Acct > Auth and Acct Setup (continued)

LABEL	DESCRIPTION
Login	These fields specify which database the Switch should use (first, second and third) to authenticate administrator accounts (users for Switch management). Configure the local user accounts in the **Access Control > Logins** screen. The TACACS+ and RADIUS are external servers. Before you specify the priority, make sure you have set up the corresponding database correctly first. You can specify up to three methods for the Switch to authenticate administrator accounts. The Switch checks the methods in the order you configure them (first **Method 1**, then **Method 2** and finally **Method 3**). You must configure the settings in the **Method 1** field. If you want the Switch to check other sources for administrator accounts, specify them in **Method 2** and **Method 3** fields. Select **local** to have the Switch check the administrator accounts configured in the **Access Control > Logins** screen. Select **radius** to have the Switch check the administrator accounts configured via the RADIUS Server. Select **tacacs+** to have the Switch check the administrator accounts configured via the TACACS+ Server**.**
Accounting	Use this section to configure accounting settings on the Switch.
Update Period	This is the amount of time in minutes before the Switch sends an update to the accounting server. This is only valid if you select the **start-stop** option for the **Exec** or **Dot1x** entries.
Type	The Switch supports the following types of events to be sent to the accounting server(s): • **System** - Configure the Switch to send information when the following system events occur: system boots up, system shuts down, system accounting is enabled, system accounting is disabled • **Exec** - Configure the Switch to send information when an administrator logs in and logs out via the console port, telnet or SSH. • **Dot1x** - Configure the Switch to send information when an IEEE 802.1x client begins a session (authenticates via the Switch), ends a session as well as interim updates of a session. • **Commands** - Configure the Switch to send information when commands of specified privilege level and higher are executed on the Switch.
Active	Select this to activate accounting for a specified event types.
Broadcast	Select this to have the Switch send accounting information to all configured accounting servers at the same time. If you don't select this and you have two accounting servers set up, then the Switch sends information to the first accounting server and if it doesn't get a response from the accounting server then it tries the second accounting server.
Mode	The Switch supports two modes of recording login events. Select: • **start-stop** - to have the Switch send information to the accounting server when a user begins a session, during a user's session (if it lasts past the **Update Period**), and when a user ends a session. • **stop-only** - to have the Switch send information to the accounting server only when a user ends a session.
Method	Select whether you want to use RADIUS or TACACS+ for accounting of specific types of events. TACACS+ is the only method for recording **Commands** type of event.
Privilege	This field is only configurable for **Commands** type of event. Select the threshold command privilege level for which the Switch should send accounting information. The Switch will send accounting information when commands at the level you specify and higher are executed on the Switch.

Table 64 Advanced Application > Auth and Acct > Auth and Acct Setup (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

23.2.4 Vendor Specific Attribute

RFC 2865 standard specifies a method for sending vendor-specific information between a RADIUS server and a network access device (for example, the Switch). A company can create Vendor Specific Attributes (VSAs) to expand the functionality of a RADIUS server.

The Switch supports VSAs that allow you to perform the following actions based on user authentication:

- Limit bandwidth on incoming or outgoing traffic for the port the user connects to.
- Assign account privilege levels (See Section 44.7 on page 336 for more information on account privilege levels) for the authenticated user.

The VSAs are composed of the following:

- **Vendor-ID**: An identification number assigned to the company by the IANA (Internet Assigned Numbers Authority). ZyXEL's vendor ID is 890.
- **Vendor-Type**: A vendor specified attribute, identifying the setting you want to modify.
- **Vendor-data**: A value you want to assign to the setting.

Refer to the documentation that comes with your RADIUS server on how to configure VSAs for users authenticating via the RADIUS server.

The following table describes the VSAs supported on the Switch.

Table 65 Supported VSAs

FUNCTION	ATTRIBUTE

Ingress Bandwidth Assignment	`Vendor-Id = 890`
	`Vendor-Type = 1`
	`Vendor-data =` ingress rate (Kbps in decimal format)

Table 65 Supported VSAs

FUNCTION	ATTRIBUTE
Egress Bandwidth Assignment	Vendor-Id = **890** Vendor-Type = **2** Vendor-data = egress rate (Kbps in decimal format)
Privilege Assignment	Vendor-ID = **890** Vendor-Type = **3** Vendor-Data = **"shell:priv-lvl=**N" or Vendor-ID = **9** (CISCO) Vendor-Type = **1** (CISCO-AVPAIR) Vendor-Data = **"shell:priv-lvl=**N" where N is a privilege level (from 0 to 14). Note: If you set the privilege level of a login account differently on the RADIUS server(s) and the Switch, the user is assigned a privilege level from the database (RADIUS or local) the Switch uses first for user authentication.

23.2.5 Tunnel Protocol Attribute

You can configure tunnel protocol attributes on the RADIUS server (refer to your RADIUS server documentation) to assign a port on the Switch to a VLAN based on IEEE 802.1x authentication. The port VLAN settings are fixed and untagged. This will also set the port's VID. The following table describes the values you need to configure. Note that the bolded values in the table are fixed values as defined in RFC 3580.

Table 66 Supported Tunnel Protocol Attribute

FUNCTION	ATTRIBUTE
VLAN Assignment	Tunnel-Type = **VLAN(13)** Tunnel-Medium-Type = **802(6)** Tunnel-Private-Group-ID = VLAN ID Note: You must also create a VLAN with the specified VID on the Switch.

23.3 Supported RADIUS Attributes

Remote Authentication Dial-In User Service (RADIUS) attributes are data used to define specific authentication, and accounting elements in a user profile, which is stored on the RADIUS server. This section lists the RADIUS attributes supported by the Switch.

Refer to RFC 2865 for more information about RADIUS attributes used for authentication. Refer to RFC 2866 and RFC 2869 for RADIUS attributes used for accounting.

This section lists the attributes used by authentication and accounting functions on the Switch. In cases where the attribute has a specific format associated with it, the format is specified.

23.3.1 Attributes Used for Authentication

The following sections list the attributes sent from the Switch to the RADIUS server when performing authentication.

23.3.1.1 Attributes Used for Authenticating Privilege Access

User-Name

- the format of the User-Name attribute is **$enab**#**$**, where # is the privilege level (1-14)

User-Password

NAS-Identifier

NAS-IP-Address

23.3.1.2 Attributes Used to Login Users

User-Name

User-Password

NAS-Identifier

NAS-IP-Address

23.3.1.3 Attributes Used by the IEEE 802.1x Authentication

User-Name

NAS-Identifier

NAS-IP-Address

NAS-Port

NAS-Port-Type

- This value is set to **Ethernet(15)** on the Switch.

Calling-Station-Id

Frame-MTU

EAP-Message

State

Message-Authenticator

23.3.2 Attributes Used for Accounting

The following sections list the attributes sent from the Switch to the RADIUS server when performing authentication.

23.3.2.1 Attributes Used for Accounting System Events

NAS-IP-Address

NAS-Identifier

Acct-Status-Type

Acct-Session-ID

- The format of Acct-Session-Id is **date+time+8-digit sequential number**, for example, 200704191721030000000l. (date: 2007/04/19, time: 17:21:03, serial number: 00000001)

Acct-Delay-Time

23.3.2.2 Attributes Used for Accounting Exec Events

The attributes are listed in the following table along with the time that they are sent (the difference between Console and Telnet/SSH Exec events is that the Telnet/SSH events utilize the Calling-Station-Id attribute):

Table 67 RADIUS Attributes - Exec Events via Console

ATTRIBUTE	START	INTERIM-UPDATE	STOP
User-Name	✔	✔	✔
NAS-Identifier	✔	✔	✔
NAS-IP-Address	✔	✔	✔
Service-Type	✔	✔	✔
Acct-Status-Type	✔	✔	✔
Acct-Delay-Time	✔	✔	✔
Acct-Session-Id	✔	✔	✔
Acct-Authentic	✔	✔	✔
Acct-Session-Time		✔	✔
Acct-Terminate-Cause			✔

Table 68 RADIUS Attributes - Exec Events via Telnet/SSH

ATTRIBUTE	START	INTERIM-UPDATE	STOP
User-Name	✔	✔	✔
NAS-Identifier	✔	✔	✔
NAS-IP-Address	✔	✔	✔
Service-Type	✔	✔	✔
Calling-Station-Id	✔	✔	✔
Acct-Status-Type	✔	✔	✔
Acct-Delay-Time	✔	✔	✔
Acct-Session-Id	✔	✔	✔
Acct-Authentic	✔	✔	✔
Acct-Session-Time		✔	✔
Acct-Terminate-Cause			✔

23.3.2.3 Attributes Used for Accounting IEEE 802.1x Events

The attributes are listed in the following table along with the time of the session they are sent:

Table 69 RADIUS Attributes - Exec Events via Console

ATTRIBUTE	START	INTERIM-UPDATE	STOP
User-Name	✔	✔	✔
NAS-IP-Address	✔	✔	✔
NAS-Port	✔	✔	✔
Class	✔	✔	✔
Called-Station-Id	✔	✔	✔

Table 69 RADIUS Attributes - Exec Events via Console

ATTRIBUTE	START	INTERIM-UPDATE	STOP
Calling-Station-Id	✔	✔	✔
NAS-Identifier	✔	✔	✔
NAS-Port-Type	✔	✔	✔
Acct-Status-Type	✔	✔	✔
Acct-Delay-Time	✔	✔	✔
Acct-Session-Id	✔	✔	✔
Acct-Authentic	✔	✔	✔
Acct-Input-Octets		✔	✔
Acct-Output-Octets		✔	✔
Acct-Session-Time		✔	✔
Acct-Input-Packets		✔	✔
Acct-Output-Packets		✔	✔
Acct-Terminate-Cause			✔
Acct-Input-Gigawords		✔	✔
Acct-Output-Gigawords		✔	✔

24

IP Source Guard

Use IP source guard to filter unauthorized DHCP and ARP packets in your network.

24.1 IP Source Guard Overview

IP source guard uses a binding table to distinguish between authorized and unauthorized DHCP and ARP packets in your network. A binding contains these key attributes:

- MAC address
- VLAN ID
- IP address
- Port number

When the Switch receives a DHCP or ARP packet, it looks up the appropriate MAC address, VLAN ID, IP address, and port number in the binding table. If there is a binding, the Switch forwards the packet. If there is not a binding, the Switch discards the packet.

The Switch builds the binding table by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings).

IP source guard consists of the following features:

- Static bindings. Use this to create static bindings in the binding table.
- DHCP snooping. Use this to filter unauthorized DHCP packets on the network and to build the binding table dynamically.
- ARP inspection. Use this to filter unauthorized ARP packets on the network.

If you want to use dynamic bindings to filter unauthorized ARP packets (typical implementation), you have to enable DHCP snooping before you enable ARP inspection.

24.1.1 DHCP Snooping Overview

Use DHCP snooping to filter unauthorized DHCP packets on the network and to build the binding table dynamically. This can prevent clients from getting IP addresses from unauthorized DHCP servers.

24.1.1.1 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for DHCP snooping. This setting is independent of the trusted/untrusted setting for ARP inspection. You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second.

Trusted ports are connected to DHCP servers or other switches. The Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. The Switch learns dynamic bindings from trusted ports.

The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.

Untrusted ports are connected to subscribers. The Switch discards DHCP packets from untrusted ports in the following situations:

- The packet is a DHCP server packet (for example, OFFER, ACK, or NACK).
- The source MAC address and source IP address in the packet do not match any of the current bindings.
- The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings.
- The rate at which DHCP packets arrive is too high.

24.1.1.2 DHCP Snooping Database

The Switch stores the binding table in volatile memory. If the Switch restarts, it loads static bindings from permanent memory but loses the dynamic bindings, in which case the devices in the network have to send DHCP requests again. As a result, it is recommended you configure the DHCP snooping database.

The DHCP snooping database maintains the dynamic bindings for DHCP snooping and ARP inspection in a file on an external TFTP server. If you set up the DHCP snooping database, the Switch can reload the dynamic bindings from the DHCP snooping database after the Switch restarts.

You can configure the name and location of the file on the external TFTP server. The file has the following format:

Figure 98 DHCP Snooping Database File Format

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<binding-1> <checksum-1>
<binding-2> <checksum-1-2>
...
...
<binding-n> <checksum-1-2-..-n>
END
```

The <initial-checksum> helps distinguish between the bindings in the latest update and the bindings from previous updates. Each binding consists of 72 bytes, a space, and another checksum that is used to validate the binding when it is read. If the calculated checksum is not equal to the checksum in the file, that binding and all others after it are ignored.

24.1.1.3 DHCP Relay Option 82 Information

The Switch can add information to DHCP requests that it does not discard. This provides the DHCP server more information about the source of the requests. The Switch can add the following information:

- Slot ID (1 byte), port ID (1 byte), and source VLAN ID (2 bytes)
- System name (up to 32 bytes)

This information is stored in an Agent Information field in the option 82 field of the DHCP headers of client DHCP request frames. See Chapter 32 on page 259 for more information about DHCP relay option 82.

When the DHCP server responds, the Switch removes the information in the Agent Information field before forwarding the response to the original source.

You can configure this setting for each source VLAN. This setting is independent of the DHCP relay settings (Chapter 32 on page 259).

24.1.1.4 Configuring DHCP Snooping

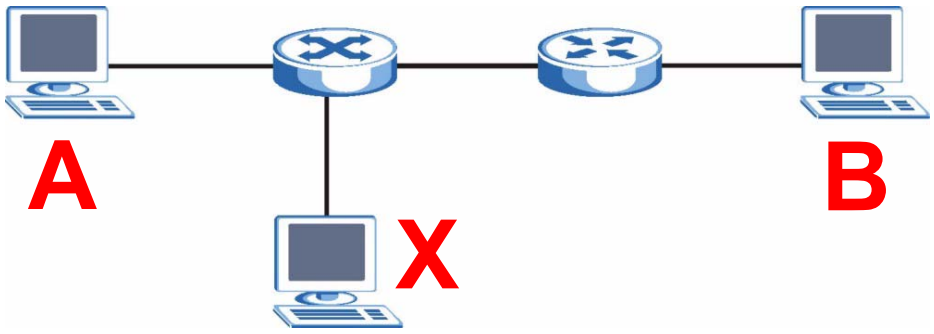
Follow these steps to configure DHCP snooping on the Switch.

1. Enable DHCP snooping on the Switch.
2. Enable DHCP snooping on each VLAN, and configure DHCP relay option 82.
3. Configure trusted and untrusted ports, and specify the maximum number of DHCP packets that each port can receive per second.
4. Configure static bindings.

24.1.2 ARP Inspection Overview

Use ARP inspection to filter unauthorized ARP packets on the network. This can prevent many kinds of man-in-the-middle attacks, such as the one in the following example.

Figure 99 Example: Man-in-the-middle Attack



In this example, computer **B** tries to establish a connection with computer **A**. Computer **X** is in the same broadcast domain as computer **A** and intercepts the ARP request for computer **A**. Then, computer **X** does the following things:

- It pretends to be computer **A** and responds to computer **B**.
- It pretends to be computer **B** and sends a message to computer **A**.

As a result, all the communication between computer **A** and computer **B** passes through computer **X**. Computer **X** can read and alter the information passed between them.

24.1.2.1 ARP Inspection and MAC Address Filters

When the Switch identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet. You can configure how long the MAC address filter remains in the Switch.

These MAC address filters are different than regular MAC address filters (Chapter 10 on page 105).

- They are stored only in volatile memory.
- They do not use the same space in memory that regular MAC address filters use.
- They appear only in the **ARP Inspection** screens and commands, not in the **MAC Address Filter** screens and commands.

24.1.2.2 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for ARP inspection. This setting is independent of the trusted/untrusted setting for DHCP snooping. You can also specify the maximum rate at which the Switch receives ARP packets on untrusted ports.

The Switch does not discard ARP packets on trusted ports for any reason.

The Switch discards ARP packets on untrusted ports in the following situations:

- The sender's information in the ARP packet does not match any of the current bindings.
- The rate at which ARP packets arrive is too high.

24.1.2.3 Syslog

The Switch can send syslog messages to the specified syslog server (Chapter 37 on page 305) when it forwards or discards ARP packets. The Switch can consolidate log messages and send log messages in batches to make this mechanism more efficient.

24.1.2.4 Configuring ARP Inspection

Follow these steps to configure ARP inspection on the Switch.

1. Configure DHCP snooping. See Section 24.1.1.4 on page 203.

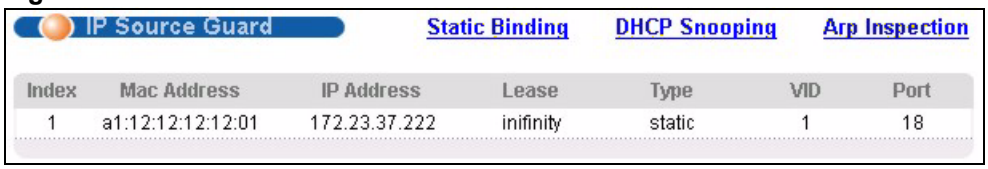
It is recommended you enable DHCP snooping at least one day before you enable ARP inspection so that the Switch has enough time to build the binding table.

2. Enable ARP inspection on each VLAN.
3. Configure trusted and untrusted ports, and specify the maximum number of ARP packets that each port can receive per second.

24.2 IP Source Guard

Use this screen to look at the current bindings for DHCP snooping and ARP inspection. Bindings are used by DHCP snooping and ARP inspection to distinguish between authorized and unauthorized packets in the network. The Switch learns the bindings by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings). To open this screen, click **Advanced Application > IP Source Guard**.

Figure 100 IP Source Guard



The following table describes the labels in this screen.

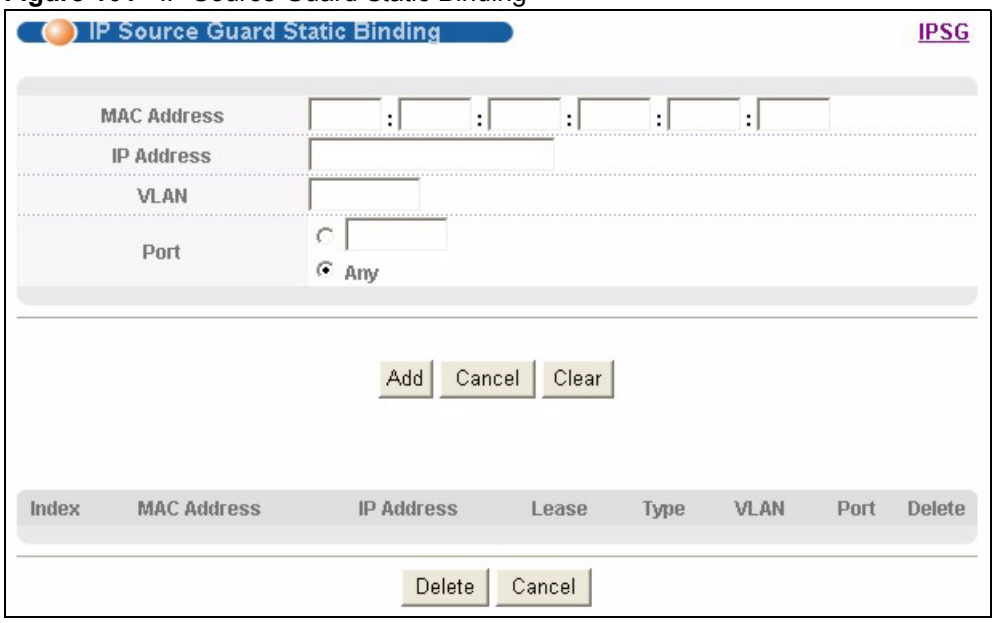
Table 70 IP Source Guard

LABEL	DESCRIPTION
Index	This field displays a sequential number for each binding.
MAC Address	This field displays the source MAC address in the binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Lease	This field displays how many days, hours, minutes, and seconds the binding is valid; for example, **2d3h4m5s** means the binding is still valid for 2 days, 3 hours, 4 minutes and 5 seconds. This field displays **infinity** if the binding is always valid (for example, a static binding).
Type	This field displays how the Switch learned the binding. **static**: This binding was learned from information provided manually by an administrator. **dhcp-snooping**: This binding was learned by snooping DHCP packets.
VID	This field displays the source VLAN ID in the binding.
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.

24.3 IP Source Guard Static Binding

Use this screen to manage static bindings for DHCP snooping and ARP inspection. Static bindings are uniquely identified by the MAC address and VLAN ID. Each MAC address and VLAN ID can only be in one static binding. If you try to create a static binding with the same MAC address and VLAN ID as an existing static binding, the new static binding replaces the original one. To open this screen, click **Advanced Application > IP Source Guard > Static Binding**.

Figure 101 IP Source Guard Static Binding



The following table describes the labels in this screen.

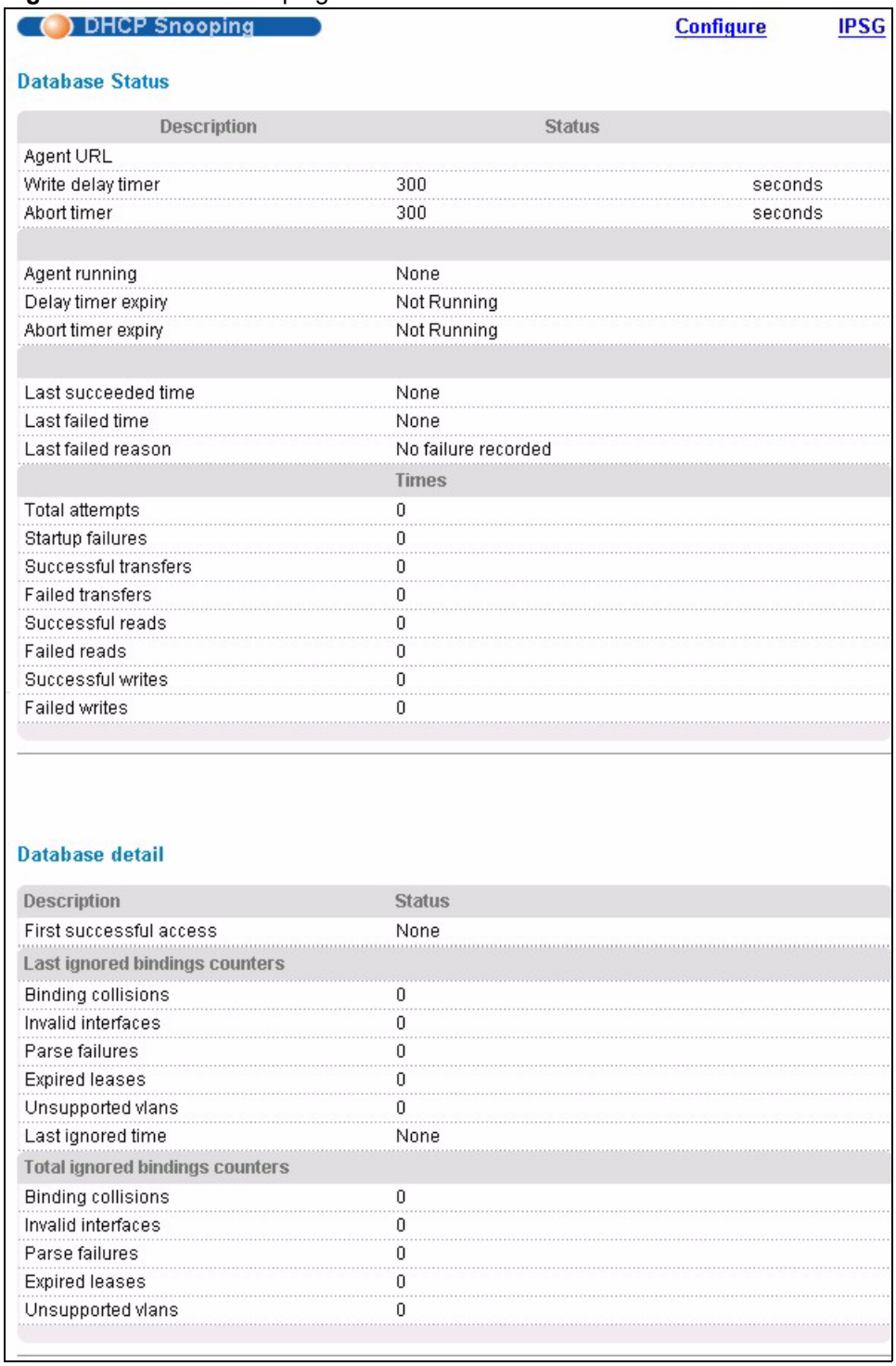
Table 71 IP Source Guard Static Binding

LABEL	DESCRIPTION
MAC Address	Enter the source MAC address in the binding.
IP Address	Enter the IP address assigned to the MAC address in the binding.
VLAN	Enter the source VLAN ID in the binding.
Port	Specify the port(s) in the binding. If this binding has one port, select the first radio button and enter the port number in the field to the right. If this binding applies to all ports, select **Any**.
Add	Click this to create the specified static binding or to update an existing one.
Cancel	Click this to reset the values above based on the last selected static binding or, if not applicable, to clear the fields above.
Clear	Click this to clear the fields above.
Index	This field displays a sequential number for each binding.
MAC Address	This field displays the source MAC address in the binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Lease	This field displays how long the binding is valid.
Type	This field displays how the Switch learned the binding. **static**: This binding was learned from information provided manually by an administrator.
VLAN	This field displays the source VLAN ID in the binding.
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.
Delete	Select this, and click **Delete** to remove the specified entry.
Cancel	Click this to clear the **Delete** check boxes above.

24.4 DHCP Snooping

Use this screen to look at various statistics about the DHCP snooping database. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping**.

Figure 102 DHCP Snooping



The following table describes the labels in this screen.

Table 72 DHCP Snooping

LABEL	DESCRIPTION
Database Status	
	This section displays the current settings for the DHCP snooping database. You can configure them in the **DHCP Snooping Configure** screen. See Section 24.5 on page 210.
Agent URL	This field displays the location of the DHCP snooping database.
Write delay timer	This field displays how long (in seconds) the Switch tries to complete a specific update in the DHCP snooping database before it gives up.
Abort timer	This field displays how long (in seconds) the Switch waits to update the DHCP snooping database after the current bindings change.
	This section displays information about the current update and the next update of the DHCP snooping database.
Agent running	This field displays the status of the current update or access of the DHCP snooping database. **none**: The Switch is not accessing the DHCP snooping database. **read**: The Switch is loading dynamic bindings from the DHCP snooping database. **write**: The Switch is updating the DHCP snooping database.
Delay timer expiry	This field displays how much longer (in seconds) the Switch tries to complete the current update before it gives up. It displays **Not Running** if the Switch is not updating the DHCP snooping database right now.
Abort timer expiry	This field displays when (in seconds) the Switch is going to update the DHCP snooping database again. It displays **Not Running** if the current bindings have not changed since the last update.
	This section displays information about the last time the Switch updated the DHCP snooping database.
Last succeeded time	This field displays the last time the Switch updated the DHCP snooping database successfully.
Last failed time	This field displays the last time the Switch updated the DHCP snooping database unsuccessfully.
Last failed reason	This field displays the reason the Switch updated the DHCP snooping database unsuccessfully.
	This section displays historical information about the number of times the Switch successfully or unsuccessfully read or updated the DHCP snooping database.
Total attempts	This field displays the number of times the Switch has tried to access the DHCP snooping database for any reason.
Startup failures	This field displays the number of times the Switch could not create or read the DHCP snooping database when the Switch started up or a new URL is configured for the DHCP snooping database.
Successful transfers	This field displays the number of times the Switch read bindings from or updated the bindings in the DHCP snooping database successfully.
Failed transfers	This field displays the number of times the Switch was unable to read bindings from or update the bindings in the DHCP snooping database.
Successful reads	This field displays the number of times the Switch read bindings from the DHCP snooping database successfully.
Failed reads	This field displays the number of times the Switch was unable to read bindings from the DHCP snooping database.

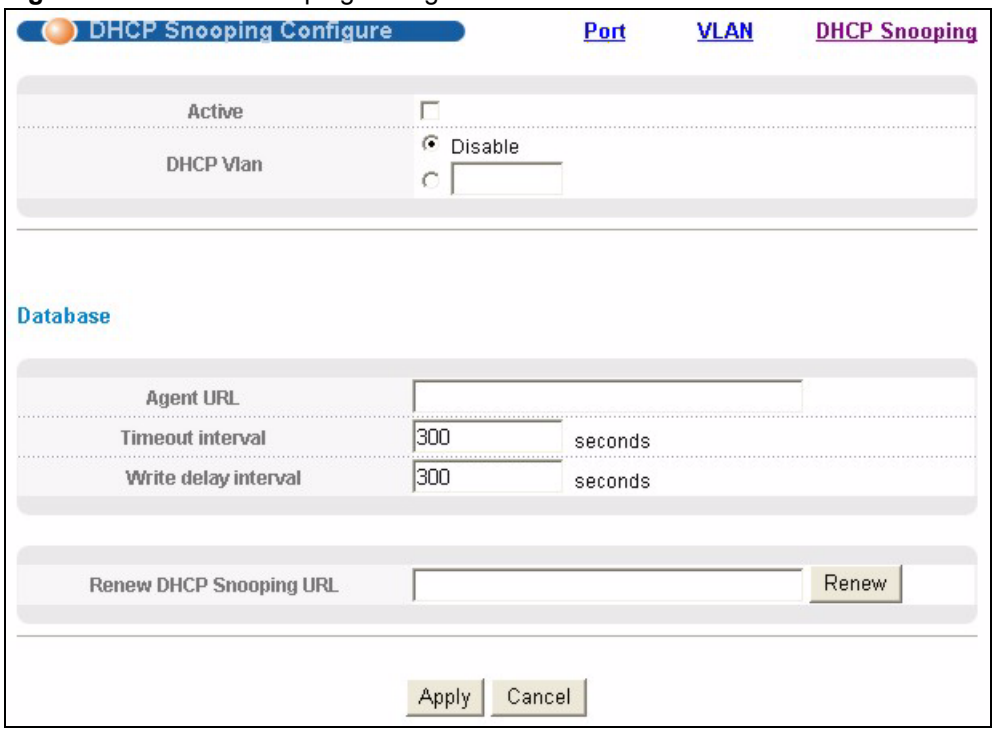
Table 72 DHCP Snooping (continued)

LABEL	DESCRIPTION
Successful writes	This field displays the number of times the Switch updated the bindings in the DHCP snooping database successfully.
Failed writes	This field displays the number of times the Switch was unable to update the bindings in the DHCP snooping database.
Database detail	
First successful access	This field displays the first time the Switch accessed the DHCP snooping database for any reason.
Last ignored bindings counters	This section displays the number of times and the reasons the Switch ignored bindings the last time it read bindings from the DHCP binding database. You can clear these counters by restarting the Switch or using CLI commands. See Chapter 44 on page 333.
Binding collisions	This field displays the number of bindings the Switch ignored because the Switch already had a binding with the same MAC address and VLAN ID.
Invalid interfaces	This field displays the number of bindings the Switch ignored because the port number was a trusted interface or does not exist anymore.
Parse failures	This field displays the number of bindings the Switch ignored because the Switch was unable to understand the binding in the DHCP binding database.
Expired leases	This field displays the number of bindings the Switch ignored because the lease time had already expired.
Unsupported vlans	This field displays the number of bindings the Switch ignored because the VLAN ID does not exist anymore.
Last ignored time	This field displays the last time the Switch ignored any bindings for any reason from the DHCP binding database.
Total ignored bindings counters	This section displays the reasons the Switch has ignored bindings any time it read bindings from the DHCP binding database. You can clear these counters by restarting the Switch or using CLI commands. See Chapter 44 on page 333.
Binding collisions	This field displays the number of bindings the Switch has ignored because the Switch already had a binding with the same MAC address and VLAN ID.
Invalid interfaces	This field displays the number of bindings the Switch has ignored because the port number was a trusted interface or does not exist anymore.
Parse failures	This field displays the number of bindings the Switch has ignored because the Switch was unable to understand the binding in the DHCP binding database.
Expired leases	This field displays the number of bindings the Switch has ignored because the lease time had already expired.
Unsupported vlans	This field displays the number of bindings the Switch has ignored because the VLAN ID does not exist anymore.

24.5 DHCP Snooping Configure

Use this screen to enable DHCP snooping on the Switch (not on specific VLAN), specify the VLAN where the default DHCP server is located, and configure the DHCP snooping database. The DHCP snooping database stores the current bindings on a secure, external TFTP server so that they are still available after a restart. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping > Configure**.

Figure 103 DHCP Snooping Configure



The following table describes the labels in this screen.

Table 73 DHCP Snooping Configure

LABEL	DESCRIPTION
Active	Select this to enable DHCP snooping on the Switch. You still have to enable DHCP snooping on specific VLAN and specify trusted ports. Note: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.
DHCP Vlan	Select a VLAN ID if you want the Switch to forward DHCP packets to DHCP servers on a specific VLAN. Note: You have to enable DHCP snooping on the DHCP VLAN too. You can enable **Option82** in the **DHCP Snooping VLAN Configure** screen (Section 24.5.2 on page 213) to help the DHCP servers distinguish between DHCP requests from different VLAN. Select **Disable** if you do not want the Switch to forward DHCP packets to a specific VLAN.

Table 73 DHCP Snooping Configure (continued)

LABEL	DESCRIPTION
Database	If **Timeout interval** is greater than **Write delay interval**, it is possible that the next update is scheduled to occur before the current update has finished successfully or timed out. In this case, the Switch waits to start the next update until it completes the current one.
Agent URL	Enter the location of the DHCP snooping database. The location should be expressed like this: **tftp://{domain name or IP address}/directory, if applicable/file name**; for example, **tftp://192.168.10.1/database.txt.**
Timeout interval	Enter how long (10-65535 seconds) the Switch tries to complete a specific update in the DHCP snooping database before it gives up.
Write delay interval	Enter how long (10-65535 seconds) the Switch waits to update the DHCP snooping database the first time the current bindings change after an update. Once the next update is scheduled, additional changes in current bindings are automatically included in the next update.
Renew DHCP Snooping URL	Enter the location of a DHCP snooping database, and click **Renew** if you want the Switch to load it. You can use this to load dynamic bindings from a different DHCP snooping database than the one specified in **Agent URL**. When the Switch loads dynamic bindings from a DHCP snooping database, it does not discard the current dynamic bindings first. If there is a conflict, the Switch keeps the dynamic binding in volatile memory and updates the **Binding collisions** counter in the **DHCP Snooping** screen (Section 24.4 on page 207).
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

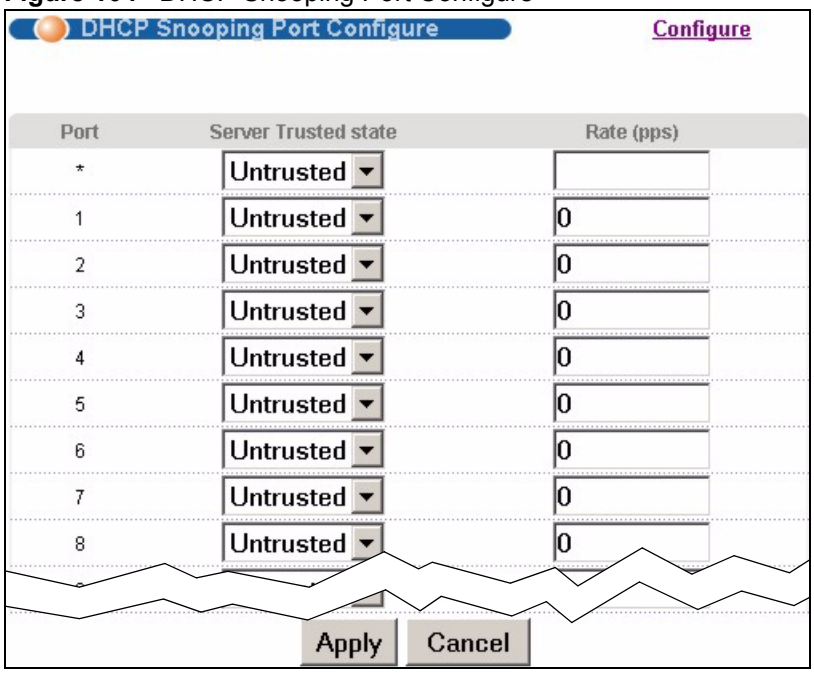
24.5.1 DHCP Snooping Port Configure

Use this screen to specify whether ports are trusted or untrusted ports for DHCP snooping.

The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.

You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping > Configure > Port**.

Figure 104 DHCP Snooping Port Configure



The following table describes the labels in this screen.

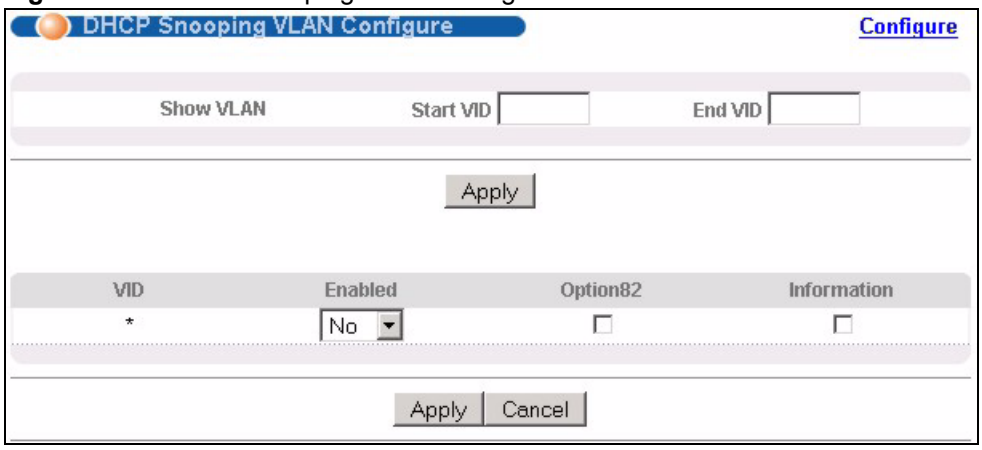
Table 74 DHCP Snooping Port Configure

LABEL	DESCRIPTION
Port	This field displays the port number. If you configure the * port, the settings are applied to all of the ports.
Server Trusted state	Select whether this port is a trusted port (**Trusted**) or an untrusted port (**Untrusted**). Trusted ports are connected to DHCP servers or other switches, and the Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. Untrusted ports are connected to subscribers, and the Switch discards DHCP packets from untrusted ports in the following situations: • The packet is a DHCP server packet (for example, OFFER, ACK, or NACK). • The source MAC address and source IP address in the packet do not match any of the current bindings. • The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings. • The rate at which DHCP packets arrive is too high.
Rate (pps)	Specify the maximum number for DHCP packets (1-2048) that the Switch receives from each port each second. The Switch discards any additional DHCP packets. Enter 0 to disable this limit, which is recommended for trusted ports.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

24.5.2 DHCP Snooping VLAN Configure

Use this screen to enable DHCP snooping on each VLAN and to specify whether or not the Switch adds DHCP relay agent option 82 information (Chapter 32 on page 259) to DHCP requests that the Switch relays to a DHCP server for each VLAN. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN**.

Figure 105 DHCP Snooping VLAN Configure



The following table describes the labels in this screen.

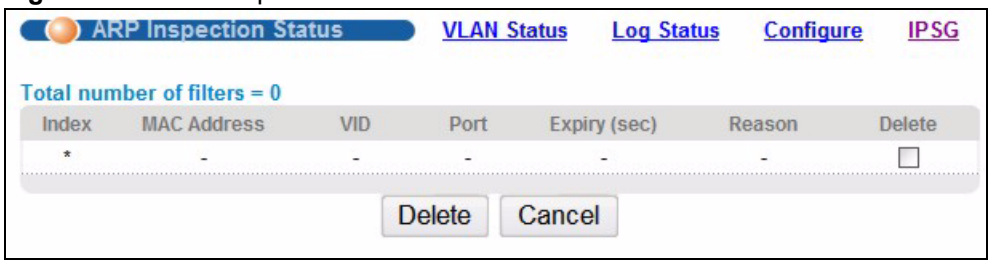
Table 75 DHCP Snooping VLAN Configure

LABEL	DESCRIPTION
Show VLAN	Use this section to specify the VLANs you want to manage in the section below.
Start VID	Enter the lowest VLAN ID you want to manage in the section below.
End VID	Enter the highest VLAN ID you want to manage in the section below.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the * VLAN, the settings are applied to all VLANs.
Enabled	Select **Yes** to enable DHCP snooping on the VLAN. You still have to enable DHCP snooping on the Switch and specify trusted ports. Note: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.
Option82	Select this to have the Switch add the slot number, port number and VLAN ID to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN. You can specify the DHCP VLAN in the **DHCP Snooping Configure** screen. See Section 24.5 on page 210.
Information	Select this to have the Switch add the system name to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN. You can configure the system name in the **General Setup** screen. See Chapter 7 on page 73. You can specify the DHCP VLAN in the **DHCP Snooping Configure** screen. See Section 24.5 on page 210.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

24.6 ARP Inspection Status

Use this screen to look at the current list of MAC address filters that were created because the Switch identified an unauthorized ARP packet. When the Switch identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection**.

Figure 106 ARP Inspection Status



The following table describes the labels in this screen.

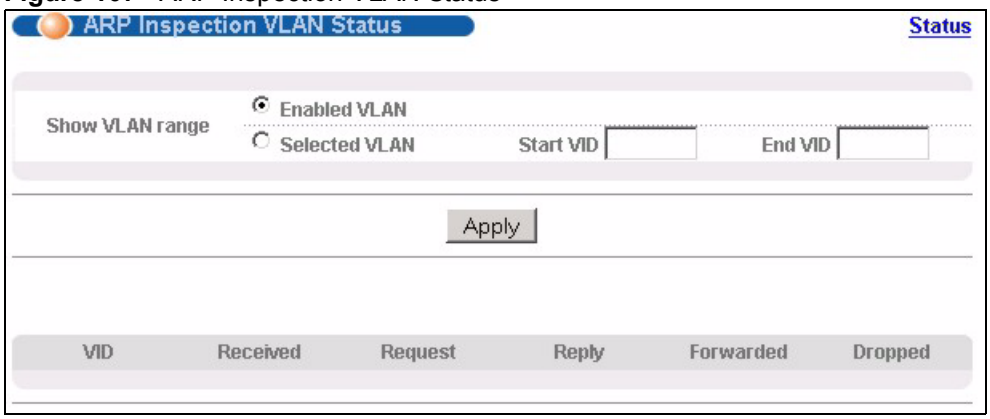
Table 76 ARP Inspection Status

LABEL	DESCRIPTION
Total number of filters	This field displays the current number of MAC address filters that were created because the Switch identified unauthorized ARP packets.
Index	This field displays a sequential number for each MAC address filter.
MAC Address	This field displays the source MAC address in the MAC address filter.
VID	This field displays the source VLAN ID in the MAC address filter.
Port	This field displays the source port of the discarded ARP packet.
Expiry (sec)	This field displays how long (in seconds) the MAC address filter remains in the Switch. You can also delete the record manually (**Delete**).
Reason	This field displays the reason the ARP packet was discarded. **MAC+VLAN**: The MAC address and VLAN ID were not in the binding table. **IP**: The MAC address and VLAN ID were in the binding table, but the IP address was not valid. **Port**: The MAC address, VLAN ID, and IP address were in the binding table, but the port number was not valid.
Delete	Select this and click **Delete** to remove the specified entry.
Delete	Click this to remove the selected entries.
Cancel	Click this to clear the **Delete** check boxes above.

24.6.1 ARP Inspection VLAN Status

Use this screen to look at various statistics about ARP packets in each VLAN. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > VLAN Status**.

Figure 107 ARP Inspection VLAN Status



The following table describes the labels in this screen.

Table 77 ARP Inspection VLAN Status

LABEL	DESCRIPTION
Show VLAN range	Use this section to specify the VLANs you want to look at in the section below.
Enabled VLAN	Select this to look at all the VLANs on which ARP inspection is enabled in the section below.
Selected VLAN	Select this to look at all the VLANs in a specific range in the section below. Then, enter the lowest VLAN ID (**Start VID**) and the highest VLAN ID (**End VID**) you want to look at.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above.
Received	This field displays the total number of ARP packets received from the VLAN since the Switch last restarted.
Request	This field displays the total number of ARP Request packets received from the VLAN since the Switch last restarted.
Reply	This field displays the total number of ARP Reply packets received from the VLAN since the Switch last restarted.
Forwarded	This field displays the total number of ARP packets the Switch forwarded for the VLAN since the Switch last restarted.
Dropped	This field displays the total number of ARP packets the Switch discarded for the VLAN since the Switch last restarted.

24.6.2 ARP Inspection Log Status

Use this screen to look at log messages that were generated by ARP packets and that have not been sent to the syslog server yet. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Log Status**.

Figure 108 ARP Inspection Log Status

The following table describes the labels in this screen.

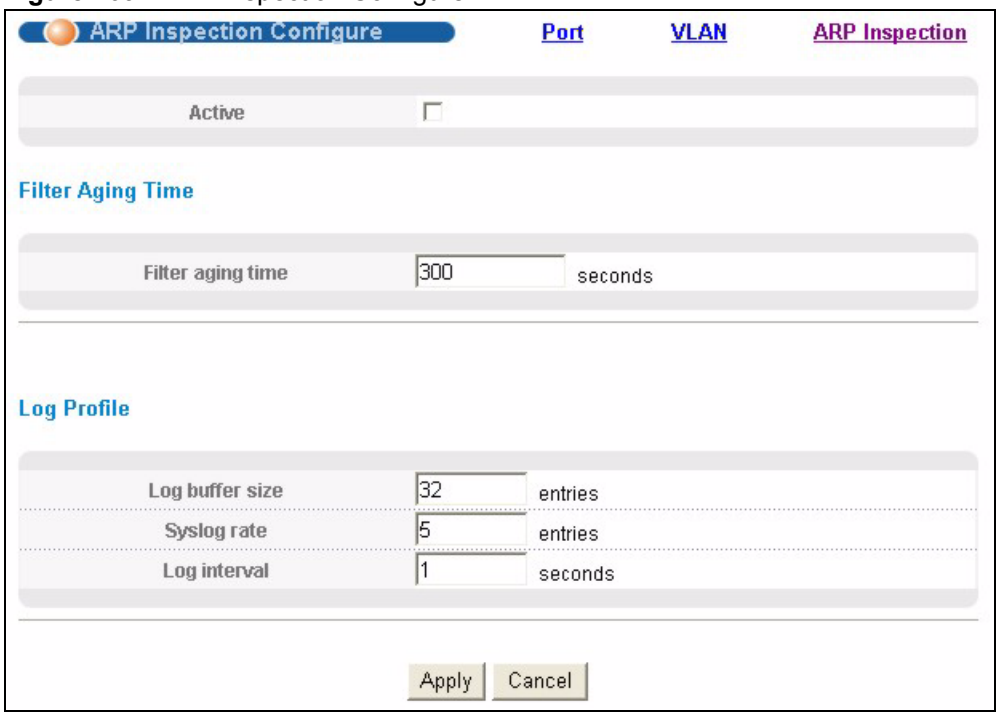
Table 78 ARP Inspection Log Status

LABEL	DESCRIPTION
Clearing log status table	Click **Apply** to remove all the log messages that were generated by ARP packets and that have not been sent to the syslog server yet.
Total number of logs	This field displays the number of log messages that were generated by ARP packets and that have not been sent to the syslog server yet. If one or more log messages are dropped due to unavailable buffer, there is an entry called **overflow** with the current number of dropped log messages.
Index	This field displays a sequential number for each log message.
Port	This field displays the source port of the ARP packet.
VID	This field displays the source VLAN ID of the ARP packet.
Sender Mac	This field displays the source MAC address of the ARP packet.
Sender IP	This field displays the source IP address of the ARP packet.
Num Pkts	This field displays the number of ARP packets that were consolidated into this log message. The Switch consolidates identical log messages generated by ARP packets in the log consolidation interval into one log message. You can configure this interval in the **ARP Inspection Configure** screen. See Section 24.7 on page 217.
Reason	This field displays the reason the log message was generated. **dhcp deny**: An ARP packet was discarded because it violated a dynamic binding with the same MAC address and VLAN ID. **static deny**: An ARP packet was discarded because it violated a static binding with the same MAC address and VLAN ID. **deny**: An ARP packet was discarded because there were no bindings with the same MAC address and VLAN ID. **dhcp permit**: An ARP packet was forwarded because it matched a dynamic binding. **static permit**: An ARP packet was forwarded because it matched a static binding. In the **ARP Inspection VLAN Configure** screen, you can configure the Switch to generate log messages when ARP packets are discarded or forwarded based on the VLAN ID of the ARP packet. See Section 24.7.2 on page 219.
Time	This field displays when the log message was generated.

24.7 ARP Inspection Configure

Use this screen to enable ARP inspection on the Switch. You can also configure the length of time the Switch stores records of discarded ARP packets and global settings for the ARP inspection log. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure**.

Figure 109 ARP Inspection Configure



The following table describes the labels in this screen.

Table 79 ARP Inspection Configure

LABEL	DESCRIPTION
Active	Select this to enable ARP inspection on the Switch. You still have to enable ARP inspection on specific VLAN and specify trusted ports.
Filter Aging Time	
Filter aging time	This setting has no effect on existing MAC address filters. Enter how long (1-2147483647 seconds) the MAC address filter remains in the Switch after the Switch identifies an unauthorized ARP packet. The Switch automatically deletes the MAC address filter afterwards. Type 0 if you want the MAC address filter to be permanent.
Log Profile	
Log buffer size	Enter the maximum number (1-1024) of log messages that were generated by ARP packets and have not been sent to the syslog server yet. Make sure this number is appropriate for the specified **Syslog rate** and **Log interval**. If the number of log messages in the Switch exceeds this number, the Switch stops recording log messages and simply starts counting the number of entries that were dropped due to unavailable buffer. Click **Clearing log status table** in the **ARP Inspection Log Status** screen to clear the log and reset this counter. See Section 24.6.2 on page 215.

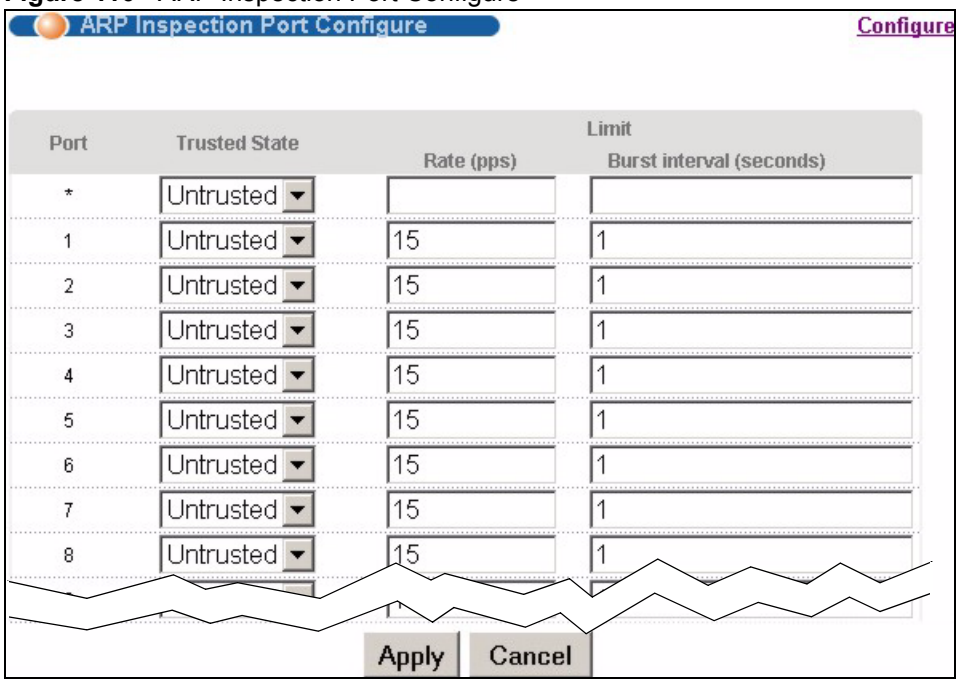
Table 79 ARP Inspection Configure (continued)

LABEL	DESCRIPTION
Syslog rate	Type the maximum number of syslog messages the Switch can send to the syslog server in one batch. This number is expressed as a rate because the batch frequency is determined by the **Log Interval**. You must configure the syslog server (Chapter 37 on page 305) to use this. Enter 0 if you do not want the Switch to send log messages generated by ARP packets to the syslog server. The relationship between **Syslog rate** and **Log interval** is illustrated in the following examples: • 4 invalid ARP packets per second, **Syslog rate** is 5, **Log interval** is 1: the Switch sends 4 syslog messages every second. • 6 invalid ARP packets per second, **Syslog rate** is 5, **Log interval** is 2: the Switch sends 10 syslog messages every 2 seconds.
Log interval	Type how often (1-86400 seconds) the Switch sends a batch of syslog messages to the syslog server. Enter 0 if you want the Switch to send syslog messages immediately. See **Syslog rate** for an example of the relationship between **Syslog rate** and **Log interval**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

24.7.1 ARP Inspection Port Configure

Use this screen to specify whether ports are trusted or untrusted ports for ARP inspection. You can also specify the maximum rate at which the Switch receives ARP packets on each untrusted port. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure > Port**.

Figure 110 ARP Inspection Port Configure



The following table describes the labels in this screen.

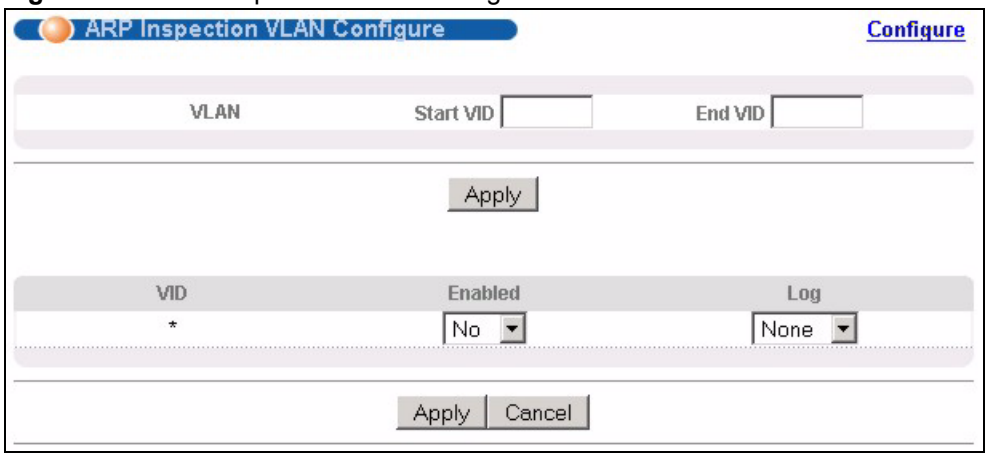
Table 80 ARP Inspection Port Configure

LABEL	DESCRIPTION
Port	This field displays the port number. If you configure the * port, the settings are applied to all of the ports.
Trusted State	Select whether this port is a trusted port (**Trusted**) or an untrusted port (**Untrusted**). The Switch does not discard ARP packets on trusted ports for any reason. The Switch discards ARP packets on untrusted ports in the following situations: • The sender's information in the ARP packet does not match any of the current bindings. • The rate at which ARP packets arrive is too high. You can specify the maximum rate at which ARP packets can arrive on untrusted ports.
Limit	Rate and Burst Interval settings have no effect on trusted ports.
Rate (pps)	Specify the maximum rate (1-2048 packets per second) at which the Switch receives ARP packets from each port. The Switch discards any additional ARP packets. Enter 0 to disable this limit.
Burst interval (seconds)	The burst interval is the length of time over which the rate of ARP packets is monitored for each port. For example, if the Rate is 15 pps and the burst interval is 1 second, then the Switch accepts a maximum of 15 ARP packets in every one-second interval. If the burst interval is 5 seconds, then the Switch accepts a maximum of 75 ARP packets in every five-second interval. Enter the length (1-15 seconds) of the burst interval.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

24.7.2 ARP Inspection VLAN Configure

Use this screen to enable ARP inspection on each VLAN and to specify when the Switch generates log messages for receiving ARP packets from each VLAN. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure > VLAN**.

Figure 111 ARP Inspection VLAN Configure



The following table describes the labels in this screen.

Table 81 ARP Inspection VLAN Configure

LABEL	DESCRIPTION
VLAN	Use this section to specify the VLANs you want to manage in the section below.
Start VID	Enter the lowest VLAN ID you want to manage in the section below.
End VID	Enter the highest VLAN ID you want to manage in the section below.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the ***** VLAN, the settings are applied to all VLANs.
Enabled	Select **Yes** to enable ARP inspection on the VLAN. Select **No** to disable ARP inspection on the VLAN.
Log	Specify when the Switch generates log messages for receiving ARP packets from the VLAN. **None**: The Switch does not generate any log messages when it receives an ARP packet from the VLAN. **Deny**: The Switch generates log messages when it discards an ARP packet from the VLAN. **Permit**: The Switch generates log messages when it forwards an ARP packet from the VLAN. **All**: The Switch generates log messages every time it receives an ARP packet from the VLAN.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

25

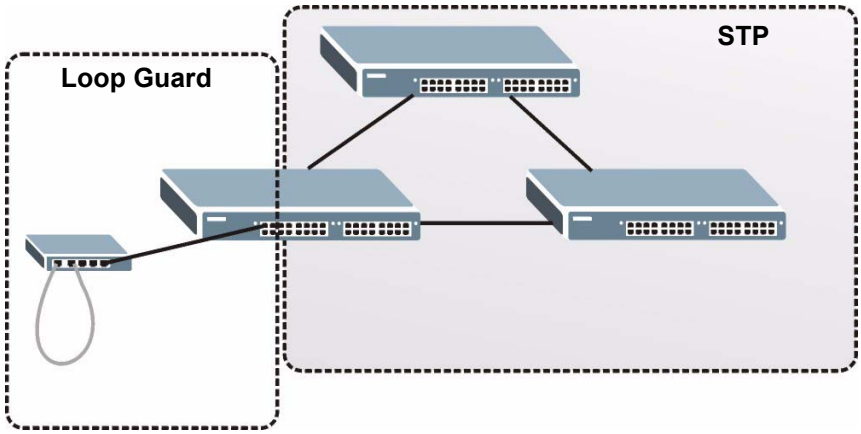
Loop Guard

This chapter shows you how to configure the Switch to guard against loops on the edge of your network.

25.1 Loop Guard Overview

Loop guard allows you to configure the Switch to shut down a port if it detects that packets sent out on that port loop back to the Switch. While you can use Spanning Tree Protocol (STP) to prevent loops in the core of your network. STP cannot prevent loops that occur on the edge of your network.

Figure 112 Loop Guard vs STP



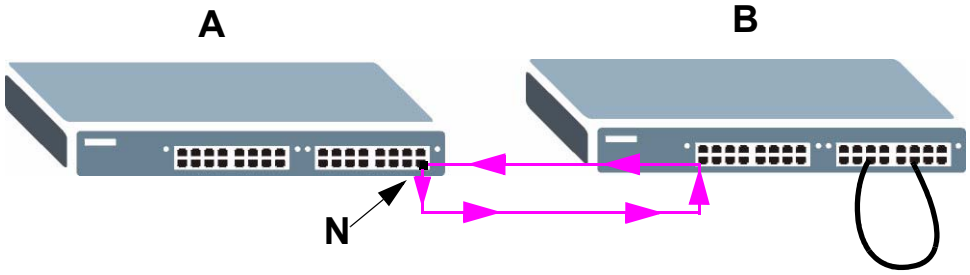
Loop guard is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a Switch that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends out broadcast messages the messages loop back to the switch and are re-broadcast again and again causing a broadcast storm.

If a switch (not in loop state) connects to a switch in loop state, then it will be affected by the switch in loop state in the following way:

- It will receive broadcast messages sent out from the switch in loop state.
- It will receive its own broadcast messages that it sends out as they loop back. It will then re-broadcast those messages again.

The following figure shows port **N** on switch **A** connected to switch **B**. Switch **B** is in loop state. When broadcast or multicast packets leave port **N** and reach switch **B**, they are sent back to port **N** on **A** as they are rebroadcast from **B**.

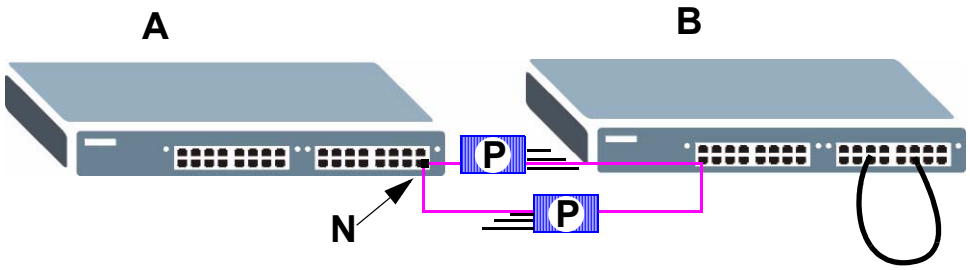
Figure 113 Switch in Loop State



The loop guard feature checks to see if a loop guard enabled port is connected to a switch in loop state. This is accomplished by periodically sending a probe packet and seeing if the packet returns on the same port. If this is the case, the Switch will shut down the port connected to the switch in loop state.

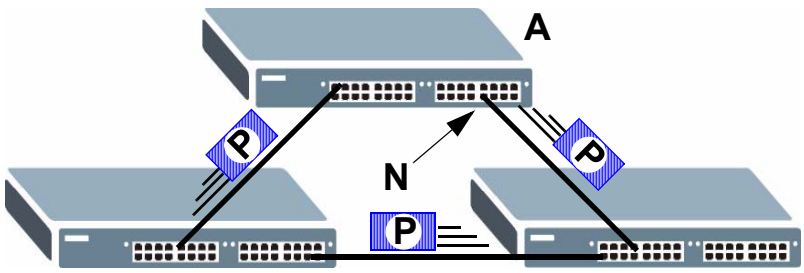
The following figure shows a loop guard enabled port **N** on switch **A** sending a probe packet **P** to switch **B**. Since switch **B** is in loop state, the probe packet **P** returns to port **N** on **A**. The Switch then shuts down port **N** to ensure that the rest of the network is not affected by the switch in loop state.

Figure 114 Loop Guard - Probe Packet



The Switch also shuts down port **N** if the probe packet returns to switch **A** on any other port. In other words loop guard also protects against standard network loops. The following figure illustrates three switches forming a loop. A sample path of the loop guard probe packet is also shown. In this example, the probe packet is sent from port **N** and returns on another port. As long as loop guard is enabled on port **N**. The Switch will shut down port **N** if it detects that the probe packet has returned to the Switch.

Figure 115 Loop Guard - Network Loop



After resolving the loop problem on your network you can re-activate the disabled port via the web configurator (see Section 7.7 on page 81) or via commands (see Section 44.12.4 on page 377).

25.2 Loop Guard Setup

Click **Advanced Application** > **Loop Guard** in the navigation panel to display the screen as shown.

The loop guard feature can not be enabled on the ports that have Spanning Tree Protocol (RSTP, MRSTP or MSTP) enabled.

Figure 116 Advanced Application > Loop Guard

The following table describes the labels in this screen.

Table 82 Advanced Application > Loop Guard

LABEL	DESCRIPTION
Active	Select this option to enable loop guard on the Switch. The Switch generates syslog, internal log messages as well as SNMP traps when it shuts down a port via the loop guard feature.
Port	This field displays a port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.

Table 82 Advanced Application > Loop Guard (continued)

LABEL	DESCRIPTION
Active	Select this check box to enable the loop guard feature on this port. The Switch sends probe packets from this port to check if the Switch it is connected to is in loop state. If the Switch that this port is connected is in loop state the Switch will shut down this port. Clear this check box to disable the loop guard feature.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

PART IV
IP Application

Static Route (227)
RIP (229)
OSPF (231)
IGMP (243)
DVMRP (247)
Differentiated Services (251)
DHCP (259)
VRRP (267)

26

Static Route

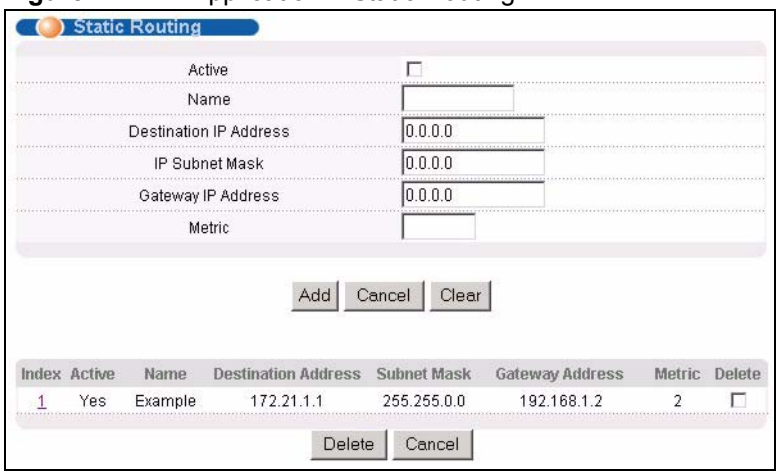
This chapter shows you how to configure static routes.

26.1 Configuring Static Routing

Static routes tell the Switch how to forward IP traffic when you configure the TCP/IP parameters manually.

Click **IP Application** > **Static Routing** in the navigation panel to display the screen as shown.

Figure 117 IP Application > Static Routing



The following table describes the related labels you use to create a static route.

Table 83 IP Application > Static Routing

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination. The gateway must be a router on the same segment as your Switch.

Table 83 IP Application > Static Routing (continued)

LABEL	DESCRIPTION
Metric	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Add	Click **Add** to insert a new static route to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to set the above fields back to the factory defaults.
Index	This field displays the index number of the route. Click a number to edit the static route entry.
Active	This field displays **Yes** when the static route is activated and **NO** when it is deactivated.
Name	This field displays the descriptive name for this route. This is for identification purposes only.
Destination Address	This field displays the IP network address of the final destination.
Subnet Mask	This field displays the subnet mask for this destination.
Gateway Address	This field displays the IP address of the gateway. The gateway is the immediate neighbor of your Switch that will forward the packet to the destination.
Metric	This field displays the cost of transmission for routing purposes.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

27

RIP

This chapter shows you how to configure RIP (Routing Information Protocol).

27.1 RIP Overview

RIP (Routing Information Protocol) allows a routing device to exchange routing information with other routers. The **Direction** field controls the sending and receiving of RIP packets. When set to:

- **Both** - the Switch will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **Incoming** - the Switch will not send any RIP packets but will accept all RIP packets received.
- **Outgoing** - the Switch will send out RIP packets but will not accept any RIP packets received.
- **None** - the Switch will not send any RIP packets and will ignore any RIP packets received.

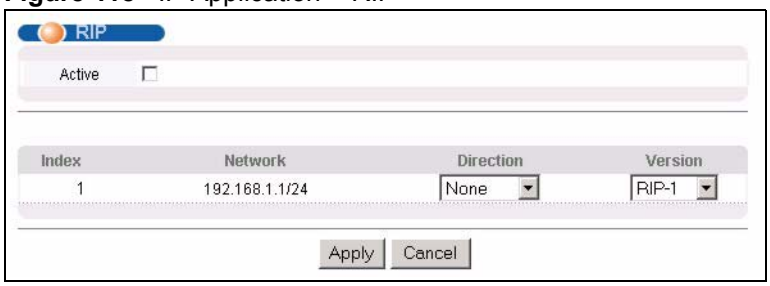
The **Version** field controls the format and the broadcasting method of the RIP packets that the Switch sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but RIP-2 carries more information. **RIP-1** is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** send the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting.

27.2 Configuring RIP

Click **IP Application** > **RIP** in the navigation panel to display the screen as shown. You cannot manually configure a new entry. Each entry in the table is automatically created when you configure a new IP domain in the **IP Setup** screen (refer to Section 7.6 on page 79).

Figure 118 IP Application > RIP



The following table describes the labels in this screen.

Table 84 IP Application > RIP

LABEL	DESCRIPTION
Active	Select this check box to enable RIP on the Switch.
Index	This field displays the index number of an IP interface.
Network	This field displays the IP interface configured on the Switch. Refer to the section on IP Setup for more information on configuring IP domains.
Direction	Select the RIP direction from the drop-down list box. Choices are **Outgoing**, **Incoming**, **Both** and **None**.
Version	Select the RIP version from the drop-down list box. Choices are **RIP-1**, **RIP-2B** and **RIP-2M**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

28

OSPF

This chapter describes the OSPF (Open Shortest Path First) routing protocol and shows you how to configure OSPF.

28.1 OSPF Overview

OSPF (Open Shortest Path First) is a link-state protocol designed to distribute routing information within an autonomous system (AS). An autonomous system is a collection of networks using a common routing protocol to exchange routing information.

OSPF offers some advantages over traditional vector-space routing protocols (such as RIP). The following table summarizes some of the major differences between OSPF and RIP.

Table 85 OSPF vs. RIP

	OSPF	RIP
Network Size	Large	Small (with up to 15 routers)
Metrics	Bandwidth, hop count, throughput, round trip time and reliability.	Hop count
Convergence	Fast	Slow

28.1.1 OSPF Autonomous Systems and Areas

An OSPF autonomous system (AS) can be divided into logical areas. Each area represents a group of adjacent networks. All areas are connected to a backbone (also known as area 0). The backbone is the transit area to route packets between two areas. A stub area, at the edge of an AS is not a transit area since there is only one connection to the stub area.

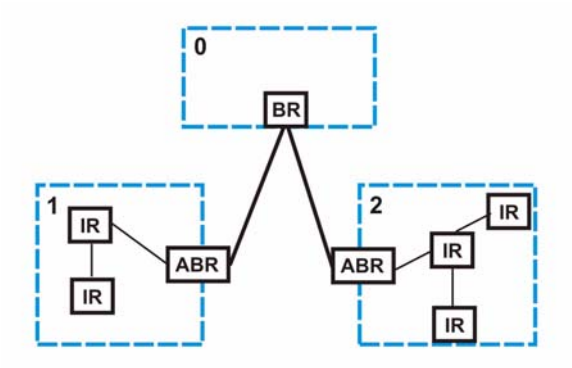
The following table describes the four classes of OSPF routers.

Table 86 OSPF: Router Types

TYPE	DESCRIPTION
Internal Router (IR)	An Internal or intra-area router is a router in an area.
Area Border Router (ABR)	An Area Border Router connects two or more areas.
Backbone Router (BR)	A backbone router has an interface to the backbone.
AS Boundary Router	An AS boundary router exchanges routing information with routers in other ASs.

The following figure depicts an OSPF network example. The backbone is area 0 with a backbone router. The internal routers are in area 1 and 2. The area border routers connect area 1 and 2 to the backbone.

Figure 119 OSPF Network Example



28.1.2 How OSPF Works

Layer 3 devices exchange routing information to build a synchronized link state database within the same AS or area. The link state database contains records of router IDs, their associated links and path costs. Each device can then use the link state database and Dijkstra algorithm to compute the least cost paths to network destinations.

Layer 3 devices build a synchronized link state database by exchanging Hello messages to confirm which neighbor (layer 3) devices exist and then they exchange database descriptions (DDs) to create the link state database. The link state database is constantly updated through LSAs (Link State Advertisements).

28.1.3 Interfaces and Virtual Links

An OSPF interface is a link between a layer 3 device and an OSPF network. An interface has state information, an IP address and subnet mask associated with it. When you configure an OSPF interface, you first set an interface to transmit OSPF traffic and add the interface to an area.

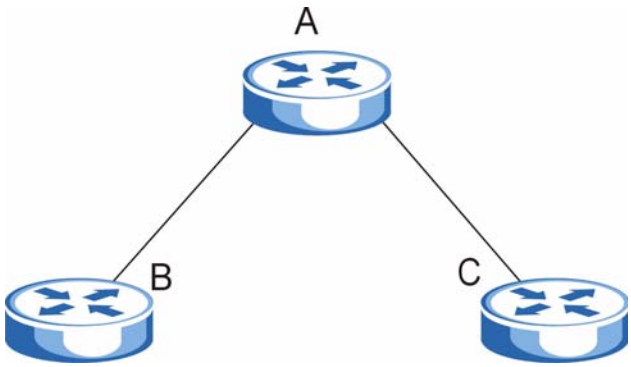
You can configure a virtual link to establish/maintain connectivity between a non-backbone area and the backbone. The virtual link must be configured on both layer 3 devices in the non-backbone area and the backbone.

28.1.4 OSPF and Router Elections

The OSPF protocol provides for automatic election of Designated Router (DR) and Backup Designated Router (BDR) on network segments. The DR and BDR keep track of link state updates in their area and make sure LSAs are sent to the rest of the network.

In most cases the default DR/BDR election is fine, but in some situations it must be controlled. In the following figure only router **A** has direct connectivity with all the other routers on the network segment. Routers **B** and **C** do not have a direct connection with each other. Therefore they should not be allowed to become DR or BDR. Only router A should become the DR.

Figure 120 OSPF Router Election Example



You can assign a priority to an interface which determines whether this router will be elected to be a DR or BDR. The router with the highest priority becomes the DR, while a router with a priority of 0 does not participate in router elections. In Figure 120 on page 233 you can assign a priority of 0 to routers **B** and **C**, thereby ensuring they do not become DR or BDR and assign a priority of 1 to router **A** to make sure that it does become the DR.

28.1.5 Configuring OSPF

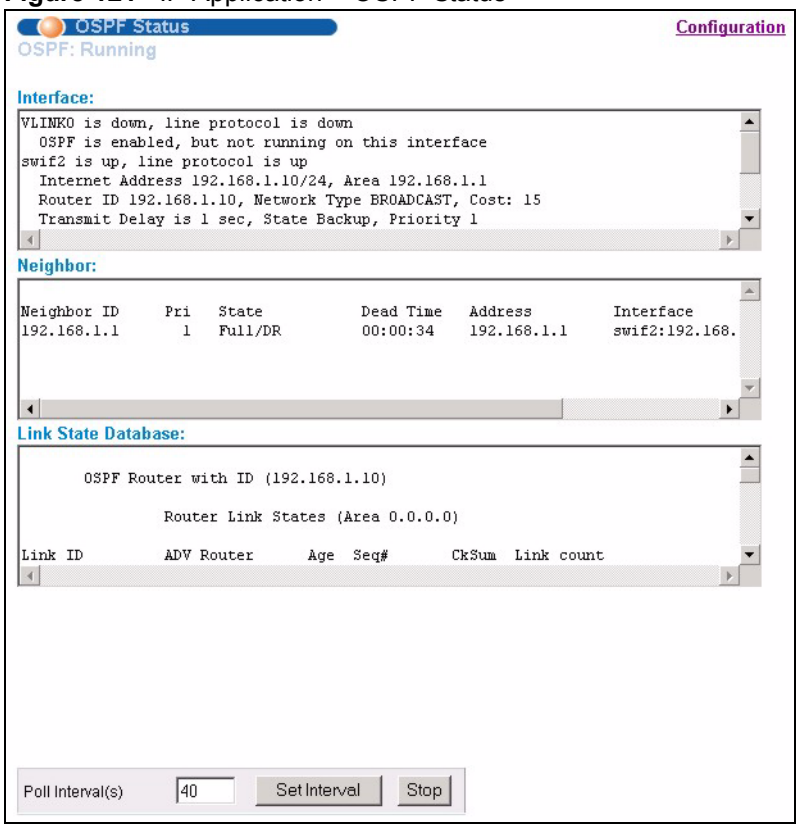
To configure OSPF on the Switch, do the following tasks

1. Enable OSPF
2. Create OSPF areas
3. Create and associate interface(s) to an area
4. Create virtual links to maintain backbone connectivity.

28.2 OSPF Status

Use this screen to view current OSPF status. Click **IP Application** > **OSPF** in the navigation panel to display the screen as shown next. See Section 28.1 on page 231 for more information on OSPF.

Figure 121 IP Application > OSPF Status


OSPF Status
Configuration
OSPF: Running
Interface:
VLINK0 is down, line protocol is down
OSPF is enabled, but not running on this interface
swif2 is up, line protocol is up
Internet Address 192.168.1.10/24, Area 192.168.1.1
Router ID 192.168.1.10, Network Type BROADCAST, Cost: 15
Transmit Delay is 1 sec, State Backup, Priority 1
Neighbor:
Neighbor ID Pri State Dead Time Address Interface
192.168.1.1 1 Full/DR 00:00:34 192.168.1.1 swif2:192.168.
Link State Database:
OSPF Router with ID (192.168.1.10)
Router Link States (Area 0.0.0.0)
Link ID ADV Router Age Seq# CkSum Link count
Poll Interval(s)
40
Set Interval
Stop

The following table describes the labels in this screen.

Table 87 IP Application > OSPF Status

LABEL	DESCRIPTION
OSPF	This field displays whether OSPF is activated (**Running**) or not (**Down**).
Interface	The text box displays the OSPF status of the interface(s) on the Switch.
Neighbor	The text box displays the status of the neighboring router participating in the OSPF network.
Link State Database	The text box displays information in the link state database which contains data in the LSAs.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to end OSPF status polling.

The following table describes some common output fields.

Table 88 OSPF Status: Common Output Fields

FIELD	DESCRIPTION
Interface	
Internet Address	This field displays the IP address and subnet bits of an IP routing domain.
Area	This field displays the area ID.
Router ID	This field displays the unique ID of the Switch.
Transmit Delay	This field displays the transmission delay in seconds.

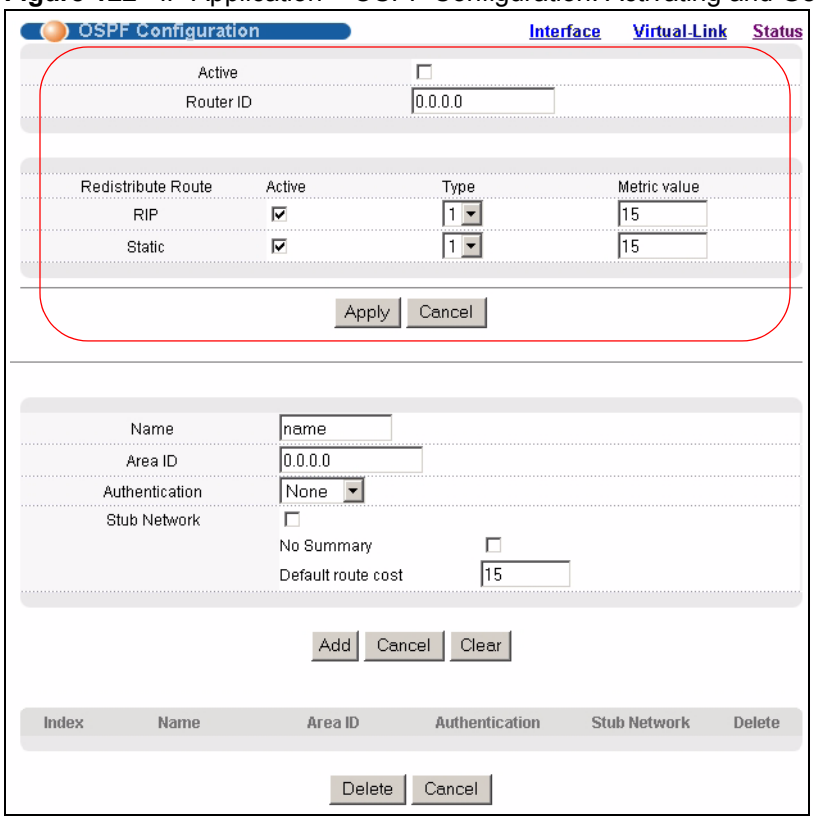
Table 88 OSPF Status: Common Output Fields (continued)

FIELD	DESCRIPTION
State	This field displays the state of the Switch (**backup** or **DR** (designated router)).
Priority	This field displays the priority of the Switch. This number is used in the designated router election.
Designated Router	This field displays the router ID of the designated router.
Backup Designated Router	This field displays the router ID of a backup designated router.
Time Intervals Configured	This field displays the time intervals (in seconds) configured.
Neighbor Count	This field displays the number of neighbor routers.
Adjacent Neighbor Count	This field displays the number of neighbor router(s) that is adjacent to the Switch.
Neighbor	
Neighbor ID	This field displays the router ID of the neighbor.
Pri	This field displays the priority of the neighbor. This number is used in the designated router election.
State	This field displays the state of the neighbor (**backup** or **DR** (designated router)).
Dead Time	This field displays the dead time in seconds.
Address	This field displays the IP address of a neighbor.
Interface	This field displays the MAC address of a device.
Link State Database	
Link ID	This field displays the ID of a router or subnet.
ADV Router	This field displays the IP address of the layer-3 device that sends the LSAs.
Age	This field displays the time (in seconds) since the last LSA was sent.
Seq #	This field displays the link sequence number of the LSA.
Checksum	This field displays the checksum value of the LSA.
Link Count	This field displays the number of links in the LSA.

28.3 OSPF Configuration

Use this screen to activate OSPF and set general settings. Click **IP Application** > **OSPF** and the **Configuration** link to display the **OSPF Configuration** screen. See Section 28.1 on page 231 for more information on OSPF.

Figure 122 IP Application > OSPF Configuration: Activating and General Settings



The follow table describes the related labels in this screen.

Table 89 IP Application > OSPF Configuration: Activating and General Settings

LABEL	DESCRIPTION
Active	OSPF is disabled by default. Select this option to enable it.
Router ID	Router ID uniquely identifies the Switch in an OSPF. Enter a unique ID (that uses the format of an IP address in dotted decimal notation) for the Switch.
Redistribute Route	Route redistribution allows your Switch to import and translate external routes learned through other routing protocols (**RIP** and **Static**) into the OSPF network transparently.
Active	Select this option to activate route redistribution for routes learned through the selected protocol.
Type	Select **1** for routing protocols (such as RIP) whose external metrics are directly comparable to the internal OSPF cost. When selecting a path, the internal OSPF cost is added to the AB boundary router to the external metrics. Select **2** for routing protocols whose external metrics are not comparable to the OSPF cost. In this case, the external cost of the AB boundary router is used in path decision to a destination.
Metric Value	Enter a route cost (between 0 and 16777214). The default **metric value** is 15.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

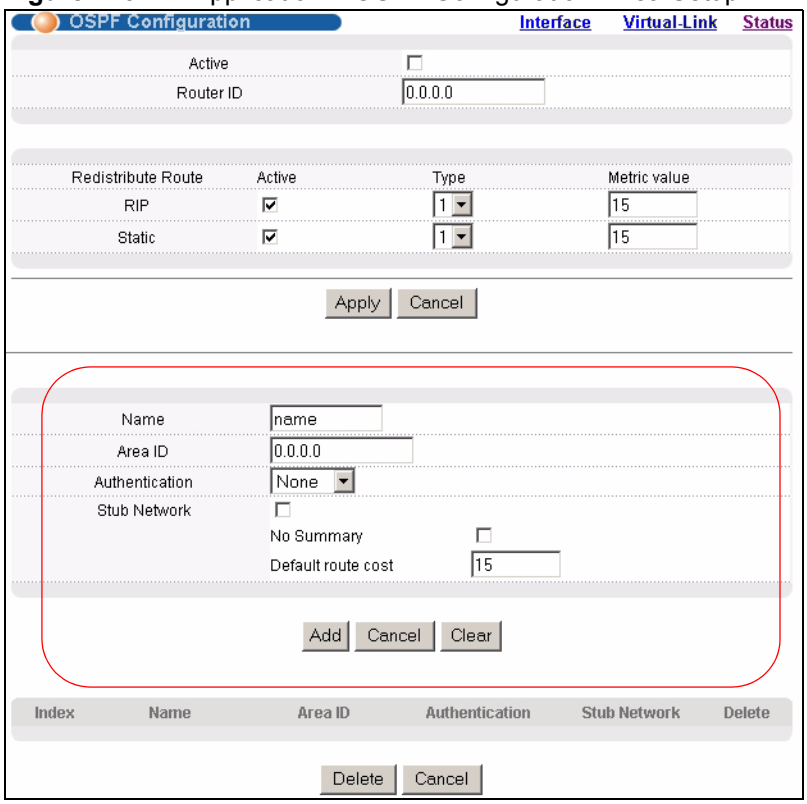
28.4 Configure OSPF Areas

To ensure that the Switch receives only routing information from a trusted layer 3 devices, activate authentication. The OSPF supports three levels of authentication:

- None – no authentication is used.
- Simple – authenticate link state updates using an 8 printable ASCII character password.
- MD5 – authenticate link state updates using a 16 printable ASCII character password.

To configure an area, set the related fields in the **OSPF Configuration** screen.

Figure 123 IP Application > OSPF Configuration: Area Setup



The following table describes the related labels in this screen.

Table 90 IP Application > OSPF Configuration: Area Setup

LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Area ID	Enter a 32-bit ID (that uses the format of an IP address in dotted decimal notation) that uniquely identifies an area. A value of **0.0.0.0** indicates that this is a backbone (also known as Area 0). You can create only one backbone area on the Switch.
Authentication	Select an authentication method (**Simple** or **MD5**) to activate authentication. Select **None** (default) to disable authentication. Usually interface(s) and virtual interface(s) should use the same authentication method as the associated area. If interface(s) and virtual interface(s) use different authentication methods than the associated area, the authentication methods are based on the interface(s) and virtual interface(s) settings.

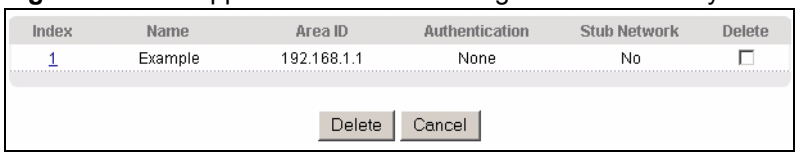
Table 90 IP Application > OSPF Configuration: Area Setup (continued)

LABEL	DESCRIPTION
Stub Network	Select this option to set the area as a stub area. If you enter **0.0.0.0** in the **Area ID** field, the settings in the **Stub Area** fields are ignored.
No Summary	Select this option to set the Switch to not send/receive LSAs.
Default Route Cost	Specify a cost (between 0 and 16777214) used to add a default route into a stub area for routes which are external to an OSPF domain. If you do not set a route cost, no default route is added.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to set the above fields back to the factory defaults.

28.4.1 View OSPF Area Information Table

The bottom of the **OSPF Configuration** screen displays a summary table of all the OSPF areas you have configured.

Figure 124 IP Application > OSPF Configuration: Summary Table



The following table describes the related labels in this screen.

Table 91 IP Application > OSPF Configuration: Summary Table

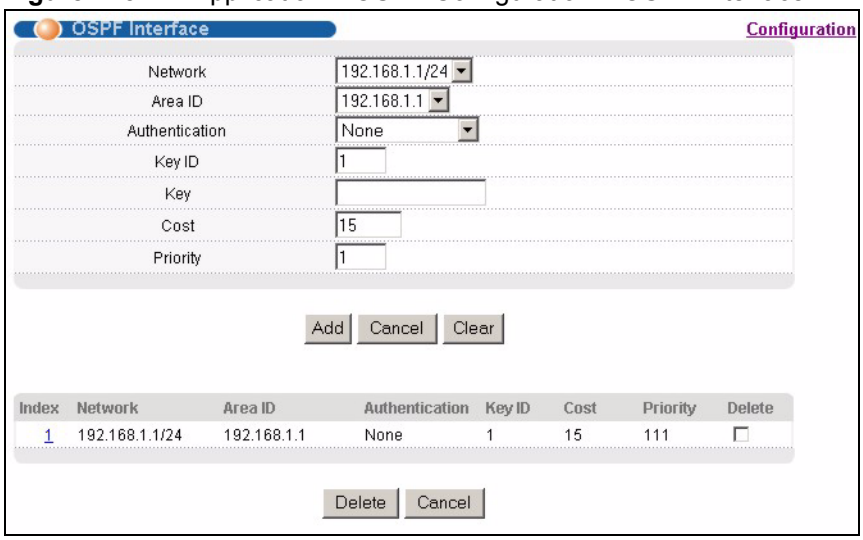
LABEL	DESCRIPTION
Index	This field displays the index number of an area.
Name	This field displays the descriptive name of an area.
Area ID	This field displays the area ID (that uses the format of an IP address in dotted decimal notation) that uniquely identifies an area. An area ID of **0.0.0.0** indicates the backbone.
Authentication	This field displays the authentication method used (**None**, **Simple** or **MD5**).
Stub Network	This field displays whether an area is a stub network (**Yes**) or not (**No**).
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

28.5 Configuring OSPF Interfaces

To configure an OSPF interface, first create an IP routing domain in the **IP Setup** screen (see Section 7.6 on page 79 for more information). Once you create an IP routing domain, an OSPF interface entry is automatically created. See Section 28.1 on page 231 for more information on OSPF.

In the **OSPF Configuration** screen, click **Interface** to display the **OSPF Interface** screen.

Figure 125 IP Application > OSPF Configuration > OSPF Interface



The following table describes the labels in this screen.

Table 92 IP Application > OSPF Configuration > OSPF Interface

LABEL	DESCRIPTION
Network	Select an IP interface.
Area ID	Select the area ID (in an IP address format with dotted decimal notation) of an area to associate the interface to that area.
Authentication	Note: OSPF Interface(s) must use the same authentication method within the same area. Select an authentication method. The choices are **Same-as-Area**, **None** (default), **Simple** and **MD5**. To participate in an OSPF network, you must make the authentication method and/or password settings the same as the associated area. Select **Same-as-Area** to use the same authentication method within the area and set the related fields when necessary. Select **None** to disable authentication. This is the default setting. Select **Simple** and set the **Key** field to authenticate OSPF packets transmitted through this interface using simple password authentication. Select **MD5** and set the **Key ID** and **Key** fields to authenticate OSPF packets transmitted through this interface using MD5 authentication.
Key ID	When you select **MD5** in the **Authentication** field, specify the identification number of the authentication you want to use.
Key	When you select **Simple** in the **Authentication** field, enter a password eight-character long. Characters after the eighth character will be ignored. When you select **MD5** in the **Authentication** field, enter a password 16-character long.
Cost	The interface cost is used for calculating the routing table. Enter a number between 0 and 65535. The default interface cost is 15.

Table 92 IP Application > OSPF Configuration > OSPF Interface (continued)

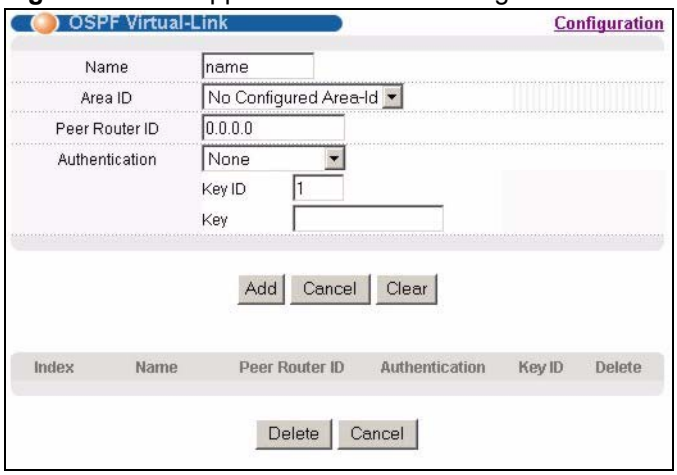
LABEL	DESCRIPTION
Priority	The priority you assign to the interface is used in router elections to decide which router is going to be the Designated Router (DR) or the Backup Designated Router (BDR). You can assign a number between 0 and 255. A priority of 0 means that the router will not participate in router elections.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to set the above fields back to the factory defaults.
Index	This field displays the index number for an interface.
Network	This field displays the IP interface information.
Area ID	This field displays the area ID (in an IP address format with dotted decimal notation) of an area to associate the interface to that area.
Authentication	This field displays the authentication method used (**Same-as-Area**, **None**, **Simple** or **MD5**).
Key ID	When the **Authentication** field displays **MD5**, this field displays the identification number of the key used.
Cost	This field displays the interface cost used for calculating the routing table.
Priority	This field displays the priority for this OSPF interface.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to begin configuring this screen afresh.

28.6 OSPF Virtual-Links

Configure and view virtual link settings in this screen. See Section 28.1 on page 231 for more information on OSPF.

In the **OSPF Configuration** screen, click **Virtual-Link** to display the screen as shown next.

Figure 126 IP Application > OSPF Configuration > OSPF Virtual Link



The following table describes the related labels in this screen.

Table 93 IP Application > OSPF Configuration > OSPF Virtual Link

LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Area ID	Select the area ID (in an IP address format with dotted decimal notation) of an area to associate the interface to that area.
Peer Router ID	Enter the ID of a peer border router.
Authentication	Note: Virtual interface(s) must use the same authentication method within the same area. Select an authentication method. The choices are **Same-as-Area**, **None** (default), **Simple** and **MD5**. To exchange OSPF packets with a peer border router, you must make the authentication method and/or password settings the same as the peer border router. Select **Same-as-Area** to use the same authentication method within the area and set the related fields when necessary. Select **None** to disable authentication. This is the default setting. Select **Simple** to authenticate OSPF packets transmitted through this interface using a simple password. Select **MD5** to authenticate OSPF packets transmitted through this interface using MD5 authentication.
Key ID	When you select **MD5** in the **Authentication** field, specify the identification number of the authentication you want to use.
Key	When you select **Simple** in the **Authentication** field, enter a password eight-character long. When you select **MD5** in the **Authentication** field, enter a password 16-character long.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to set the above fields back to the factory defaults.
Index	This field displays an index number of an entry.
Name	This field displays a descriptive name of a virtual link.
Peer Router ID	This field displays the ID (that uses the format of an IP address in dotted decimal notation) of a peer border router.
Authentication	This field displays the authentication method used (**Same-as-Area**, **None**, **Simple** or **MD5**).
Key ID	When the **Authentication** field displays **MD5**, this field displays the identification number of the key used.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

29

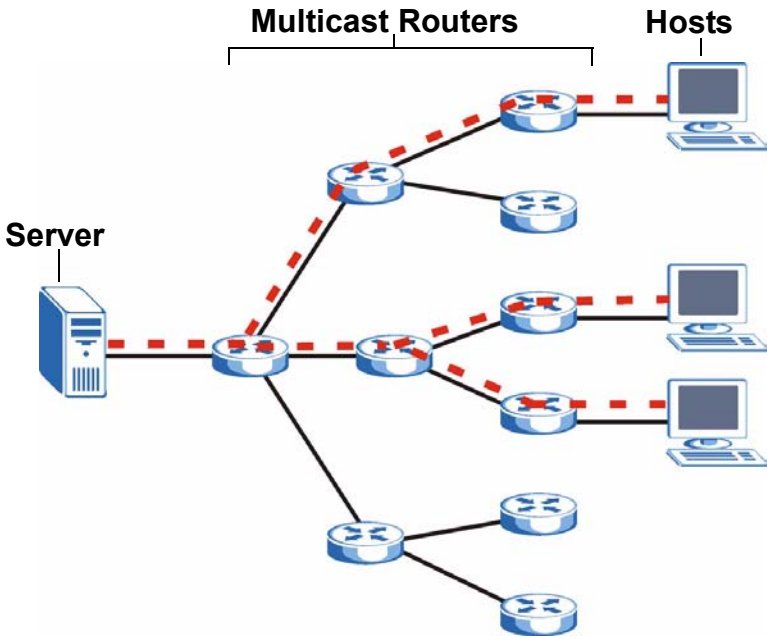
IGMP

This chapter shows you how to configure the Switch as a multicast router. See also Section 22.4 on page 177 for information on IGMP snooping.

29.1 IGMP Overview

IP multicast is an IETF standard for distributing data to multiple recipients. The following figure shows a multicast session and the relationship between a multicast server, multicast routers and multicast hosts. A multicast server transmits multicast packets and multicast routers forward multicast packets to multicast hosts.

Figure 127 IP Multicast



A host can decide to join or leave a multicast group at any time. A host can also be a member of more than one multicast group. Multicast groups are identified by IP addresses in the Class D range (224.0.0.0 to 239.255.255.255). A multicast server sends packets addressed to a particular multicast group (multicast IP address).

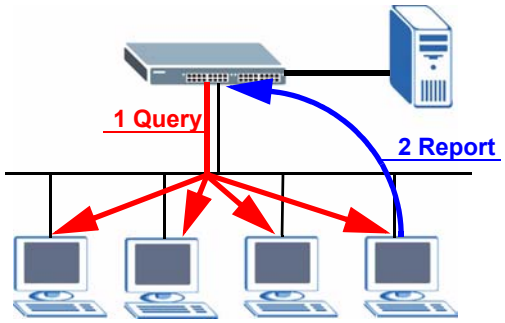
IGMP (Internet Group Management Protocol) is used by multicast hosts to indicate their multicast group membership to multicast routers. Multicast routers can also use IGMP to periodically check if multicast hosts still want to receive transmission from a multicast server. In other words, multicast routers check if any hosts on their network are still members of a specific multicast group.

The Switch supports IGMP version 1 (**IGMP-v1**), version 2 (**IGMP-v2**) and IGMP version 3 (**IGMP-v3**). Refer to RFC 1112, RFC 2236 and RFC 3376 for information on IGMP versions 1, 2 and 3 respectively. At start up, the Switch queries all directly connected networks to gather group membership. After that, the Switch periodically updates this information.

29.1.1 How IGMP Works

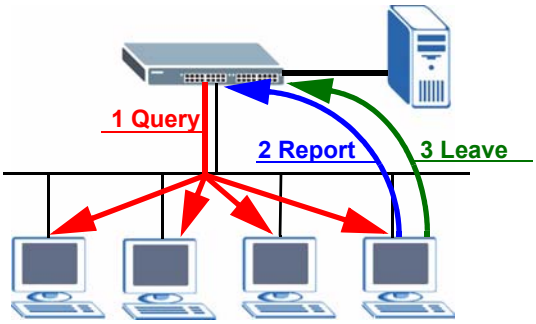
This section describes how IGMP works and the changes it has gone through from version 1 to version 3. IGMP version 1 defines how a multicast router checks to see if any multicast hosts are part of a multicast group. It checks for group membership by sending out an IGMP Query packet. Hosts that are members of a multicast group reply with an IGMP Report packet. This is also referred to as a join group request. The multicast router then keeps a list of all networks that have members of this multicast group and forwards multicast traffic to that network.

Figure 128 IGMP Version 1 Example



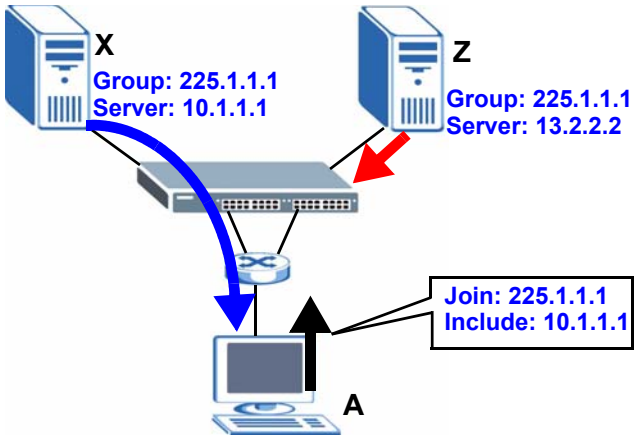
The main difference in IGMP version 2 is that it provides a mechanism for a multicast group member to notify a multicast router that it is leaving a multicast group. The multicast router then sends a group-specific IGMP query to check if there are any members remaining in that group. If the multicast router does not receive an IGMP report from any members, it stops sending multicast traffic to that group. This change helps shorten the leave convergence time, in other words, the amount of time that a multicast router believes that there are group members on a particular network. This in turn helps reduce the amount of multicast traffic going through the multicast router.

Figure 129 IGMP Version 2 Example



IGMP version 3 allows a multicast host to join a multicast group and specify from which source (multicast server) it wants to receive multicast packets. Alternatively, a multicast host can specify from which multicast servers it does not want to receive multicast packets. In the following figure multicast server **X** (IP address **10.1.1.1**) and multicast server **Z** (IP address **13.2.2.2**) both send multicast traffic to the same multicast group identified by the multicast IP address **225.1.1.1**. In IGMP version 3 multicast host **A** can join multicast group **225.1.1.1** and specify that it only wants to receive multicast packets from server **X**.

Figure 130 IGMP Version 3 Example



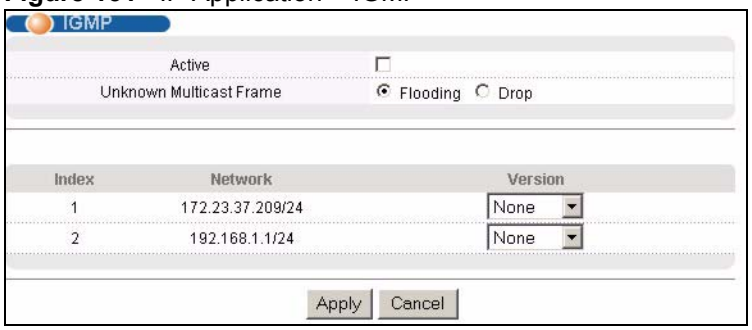
29.2 Port-based IGMP

The Switch sends IGMP Query packets to all ports. The Switch then listens for IGMP Report packets, and it records which port the messages came from. It then delivers multicast traffic to only those ports from which it received a request to join a multicast group.

29.3 Configuring IGMP

Click **IP Application** > **IGMP** in the navigation panel to display the screen as shown next. Each entry in the table is automatically created when you configure a new IP domain in the **IP Setup** screen (refer to Section 7.6 on page 79).

Figure 131 IP Application > IGMP



The following table describes the labels in this screen.

Table 94 IP Application > IGMP

LABEL	DESCRIPTION
Active	Select this check box to enable IGMP on the Switch. Note: You cannot enable both IGMP snooping and IGMP at the same time. Refer to Section 22.4 on page 177 for more information on IGMP snooping.
Unknown Multicast Frame	Specify the action to perform when the Switch receives an unknown multicast frame. Unknown multicast frames are addressed to multicast groups for which the Switch has not recorded any group members. Select **Drop** to discard the frame(s). Select **Flooding** to send the frame(s) to all ports.
Index	This field displays an index number of an entry.
Network	This field displays the IP domain configured on the Switch. Refer to Section 7.6 on page 79 for more information on configuring IP domains.
Version	Select an IGMP version from the drop-down list box. The choices are **IGMP-v1**, **IGMP-v2**, **IGMP-v3** and **None**. Generally, if you want to enable IGMP on the Switch, you should choose **IGMP-v3** as it is compatible with older versions. Choose an earlier version of IGMP (**IGMP-v2** or **IGMP-v1**) if the multicast hosts on your network can not recognize IGMP version 3 or version 2 Query messages.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

30

DVMRP

This chapter introduces DVMRP and tells you how to configure it.

30.1 DVMRP Overview

DVMRP (Distance Vector Multicast Routing Protocol) is a protocol used for routing multicast data within an autonomous system (AS). This DVMRP implementation is based on draft-ietf-idmr-dvmrp-v3-10. DVMRP provides multicast forwarding capability to a layer 3 switch that runs both the IPv4 protocol (with IP Multicast support) and the IGMP protocol. The DVMRP metric is a hop count of 32.

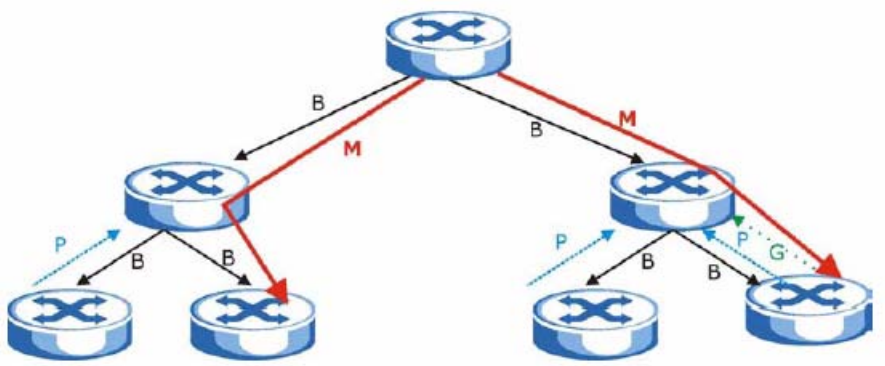
IGMP is a protocol used for joining or leaving a multicast group. You must have IGMP enabled when you enable DVMRP; otherwise you see the screen as in Figure 134 on page 249.

30.2 How DVMRP Works

DVMRP uses the Reverse Path Multicasting (RPM) algorithm to generate an IP Multicast delivery tree. Multicast packets are forwarded along these multicast tree branches. DVMRP dynamically learns host membership information using Internet Group Management Protocol (IGMP). The trees are updated dynamically to track the membership of individual groups.

1. Initially an advertisement multicast packet is broadcast ("**B**" in the following figure).
2. DVMRP-enabled Layer 3 devices that do not have any hosts in their networks that belong to this multicast group send back a prune message ("**P**").
3. If hosts later join the multicast group, a graft message ("**G**") to undo the prune is sent to the parent.
4. The final multicast ("**M**") after pruning and grafting is shown in the next figure.

Figure 132 How DVMRP Works



30.2.1 DVMRP Terminology

DVMRP probes are used to discover other DVMRP Neighbors on a network.

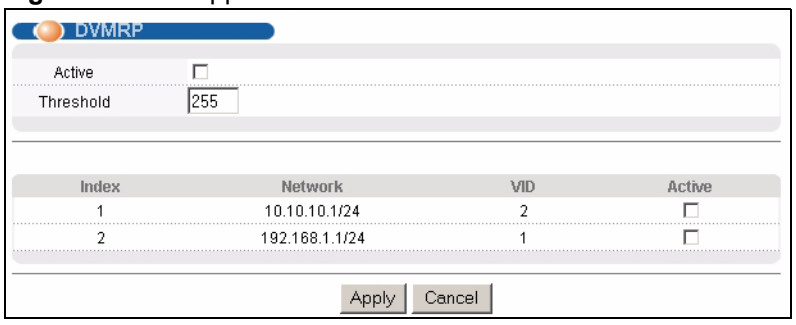
DVMRP reports are used to exchange DVMRP source routing information. These packets are used to build the DVMRP multicast routing table that is used to build source trees and also perform Reverse Path Forwarding (RPF) checks on incoming multicast packets. RPF checks prevent duplicate packets being filtered when loops exist in the network topology.

DVMRP prunes trim the multicast delivery tree(s). DVMRP grafts attach a branch back onto the multicast delivery tree.

30.3 Configuring DVMRP

Configure DVMRP on the Switch when you wish it to act as a multicast router ("mrouter"). Click **IP Application > DVMRP** in the navigation panel to display the screen as shown.

Figure 133 IP Application > DVMRP



The following table describes the labels in this screen.

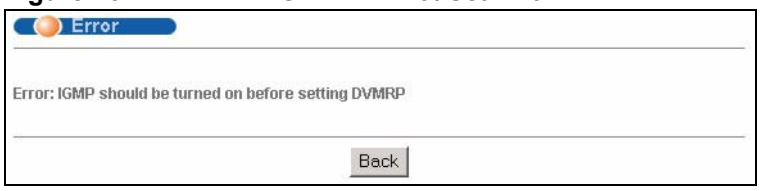
Table 95 IP Application > DVMRP

LABEL	DESCRIPTION
Active	Select **Active** to enable DVMRP on the Switch. You should do this if you want the Switch to act as a multicast router.
Threshold	Threshold is the maximum time to live (TTL) value. TTL is used to limit the scope of multicasting. You should reduce this value if you do not wish to flood Layer 3 devices many hops away with multicast traffic. This applies only to multicast traffic this Switch sends out.
Index	Index is the DVMRP configuration for the IP routing domain defined under **Network**. The maximum number of DVMRP configurations allowed is the maximum number of IP routing domains allowed on the Switch. See Section 7.6 on page 79 for more information on IP routing domains.
Network	This is the IP routing domain IP address and subnet mask you set up in **IP Setup.**
VID	DVMRP cannot be enabled on the same VLAN group across different IP routing domains, that is, you cannot have duplicate VIDs for different DVMRP configurations (see Figure 136 on page 250).
Active	Select **Active** to enable DVMRP on this IP routing domain.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

30.3.1 DVMRP Configuration Error Messages

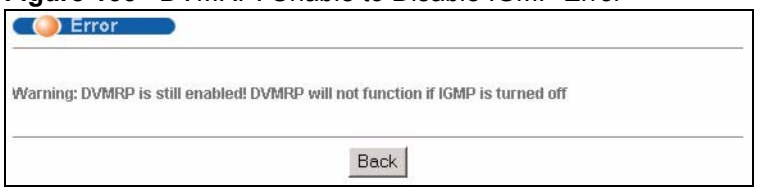
You must have IGMP/RIP enabled when you enable DVMRP; otherwise you see the screen as in the next figure.

Figure 134 DVMRP: IGMP/RIP Not Set Error



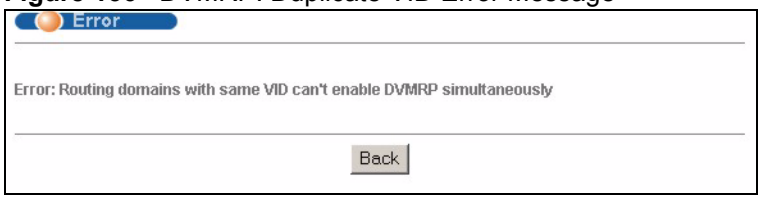
When you disable IGMP, but DVMRP is still active you also see another warning screen.

Figure 135 DVMRP: Unable to Disable IGMP Error



Each IP routing domain DVMRP configuration must be in a different VLAN group; otherwise you see the following screen.

Figure 136 DVMRP: Duplicate VID Error Message



30.4 Default DVMRP Timer Values

The following are some default DVMRP timer values.

Table 96 DVMRP: Default Timer Values

DVMRP FIELD	DEFAULT VALUE
Probe interval	10 sec
Report interval	35 sec
Route expiration time	140 sec
Prune lifetime	Variable (less than two hours)
Prune retransmission time	3 sec with exponential back off
Graft retransmission time	5 sec with exponential back off

31

Differentiated Services

This chapter shows you how to configure Differentiated Services (DiffServ) on the Switch.

31.1 DiffServ Overview

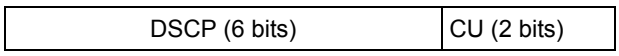
Quality of Service (QoS) is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

31.1.1 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (ToS) field in the IP header. The DS field contains a 6-bit DSCP field which can define up to 64 service levels and the remaining 2 bits are defined as currently unused (CU). The following figure illustrates the DS field.

Figure 137 DiffServ: Differentiated Service Field



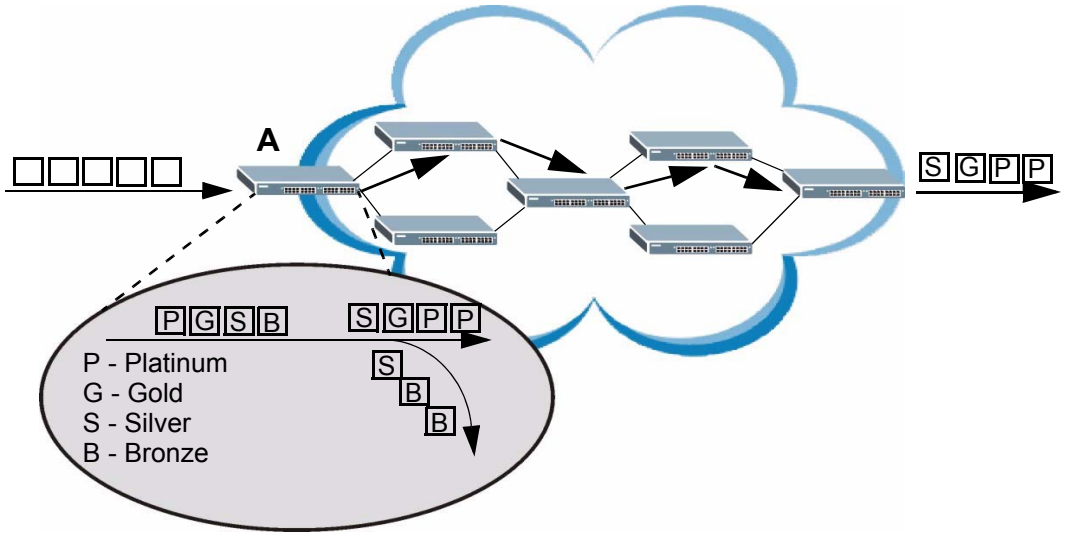
DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

The DSCP value determines the PHB (Per-Hop Behavior), that each packet gets as it is forwarded across the DiffServ network. Based on the marking rule different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

31.1.2 DiffServ Network Example

The following figure depicts a DiffServ network consisting of a group of directly connected DiffServ-compliant network devices. The boundary node (**A** in Figure 138) in a DiffServ network classifies (marks with a DSCP value) the incoming packets into different traffic flows (**Platinum**, **Gold**, **Silver**, **Bronze**) based on the configured marking rules. A network administrator can then apply various traffic policies to the traffic flows. For example, one traffic policy would be to give higher drop precedence to one traffic flow over others. In our example packets in the **Bronze** traffic flow are more likely to be dropped when congestion occurs than the packets in the **Platinum** traffic flow as they move across the DiffServ network.

Figure 138 DiffServ Network



31.2 Two Rate Three Color Marker Traffic Policing

Traffic policing is the limiting of the input or output transmission rate of a class of traffic on the basis of user-defined criteria. Traffic policing methods measure traffic flows against user-defined criteria and identify it as either conforming, exceeding or violating the criteria.

Two Rate Three Color Marker (TRTCM, defined in RFC 2698) is a type of traffic policing that identifies packets by comparing them to two user-defined rates: the Committed Information Rate (CIR) and the Peak Information Rate (PIR). The CIR specifies the average rate at which packets are admitted to the network. The PIR is greater than or equal to the CIR. CIR and PIR values are based on the guaranteed and maximum bandwidth respectively as negotiated between a service provider and client.

Two Rate Three Color Marker evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green. After TRTCM is configured and DiffServ is enabled the following actions are performed on the colored packets:

- Red (high loss priority level) packets are dropped.
- Yellow (medium loss priority level) packets are dropped if there is congestion on the network.

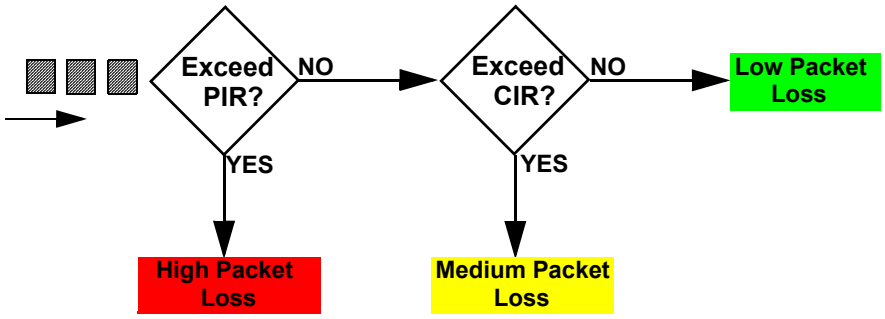
- Green (low loss priority level) packets are forwarded.

TRTCM operates in one of two modes: color-blind or color-aware. In color-blind mode, packets are marked based on evaluating against the PIR and CIR regardless of if they have previously been marked or not. In the color-aware mode, packets are marked based on both existing color and evaluation against the PIR and CIR. If the packets do not match any of colors, then the packets proceed unchanged.

31.2.1 TRTCM - Color-blind Mode

All packets are evaluated against the PIR. If a packet exceeds the PIR it is marked red. Otherwise it is evaluated against the CIR. If it exceeds the CIR then it is marked yellow. Finally, if it is below the CIR then it is marked green.

Figure 139 TRTCM - Color-blind Mode

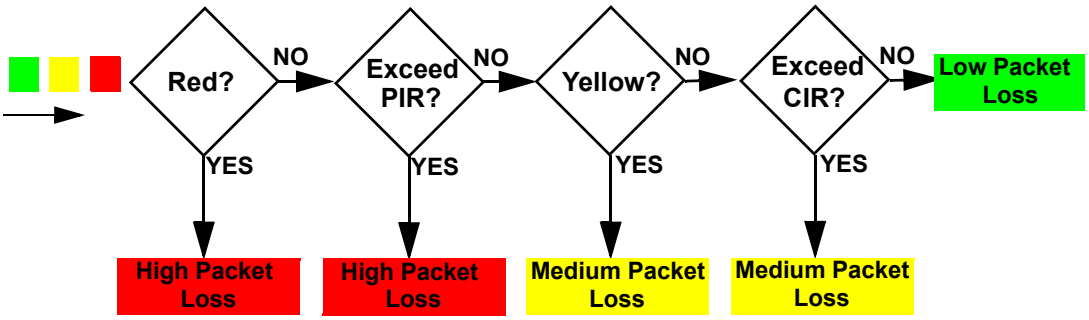


31.2.2 TRTCM - Color-aware Mode

In color-aware mode the evaluation of the packets uses the existing packet loss priority. TRTCM can increase a packet loss priority of a packet but it cannot decrease it. Packets that have been previously marked red or yellow can only be marked with an equal or higher packet loss priority.

Packets marked red (high packet loss priority) continue to be red without evaluation against the PIR or CIR. Packets marked yellow can only be marked red or remain yellow so they are only evaluated against the PIR. Only the packets marked green are first evaluated against the PIR and then if they don't exceed the PIR level are they evaluated against the CIR.

Figure 140 TRTCM - Color-aware Mode

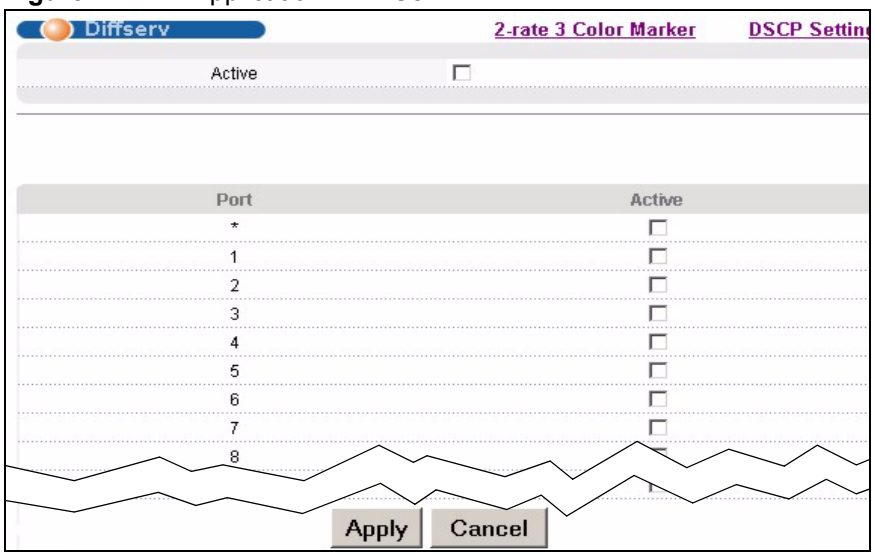


31.3 Activating DiffServ

Activate DiffServ to apply marking rules or IEEE 802.1p priority mapping on the selected port(s).

Click **IP Application** > **DiffServ** in the navigation panel to display the screen as shown.

Figure 141 IP Application > DiffServ



The following table describes the labels in this screen.

Table 97 IP Application > DiffServ

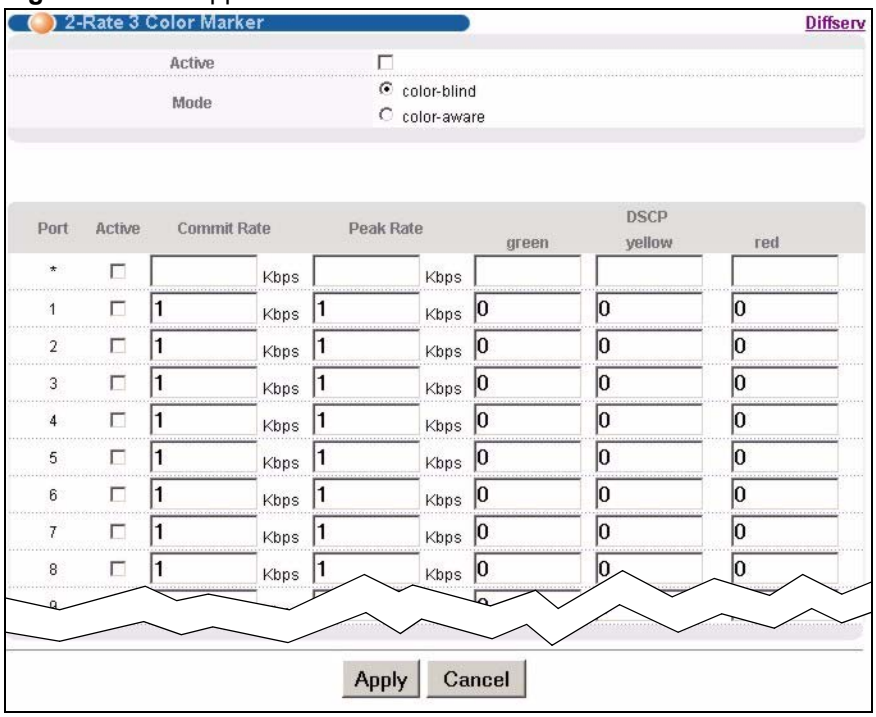
LABEL	DESCRIPTION
Active	Select this option to enable DiffServ on the Switch.
Port	This field displays the index number of a port on the Switch.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select **Active** to enable DiffServ on the port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

31.3.1 Configuring 2-Rate 3 Color Marker Settings

Use this screen to configure TRTCM settings. Click the **2-rate 3 Color Marker** link in the **DiffServ** screen to display the screen as shown next.

You cannot enable both TRTCM and Bandwidth Control at the same time.

Figure 142 IP Application > DiffServ > 2-rate 3 Color Marker



The following table describes the labels in this screen.

Table 98 IP Application > DiffServ > 2-rate 3 Color Marker

LABEL	DESCRIPTION
Active	Select this to activate TRTCM (Two Rate Three Color Marker) on the Switch. The Switch evaluates and marks the packets based on the TRTCM settings. Note: You must also activate **DiffServ** on the Switch and the individual ports for the Switch to drop red (high loss priority) colored packets.
Mode	Select **color-blind** to have the Switch treat all incoming packets as uncolored. All incoming packets are evaluated against the CIR and PIR. Select **color-aware** to treat the packets as marked by some preceding entity. Incoming packets are evaluated based on their existing color. Incoming packets that are not marked proceed through the Switch.
Port	This field displays the index number of a port on the Switch.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this to activate TRTCM on the port.
Commit Rate	Specify the Commit Information Rate (CIR) for this port.

Table 98 IP Application > DiffServ > 2-rate 3 Color Marker (continued)

LABEL	DESCRIPTION
Peak Rate	Specify the Peak Information Rate (PIR) for this port.
DSCP	Use this section to specify the DSCP values that you want to assign to packets based on the color they are marked via TRTCM.
green	Specify the DSCP value to use for packets with low packet loss priority.
yellow	Specify the DSCP value to use for packets with medium packet loss priority.
red	Specify the DSCP value to use for packets with high packet loss priority.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

31.4 DSCP-to-IEEE 802.1p Priority Settings

You can configure the DSCP to IEEE 802.1p mapping to allow the Switch to prioritize all traffic based on the incoming DSCP value according to the DiffServ to IEEE 802.1p mapping table.

The following table shows the default DSCP-to-IEEE802.1p mapping.

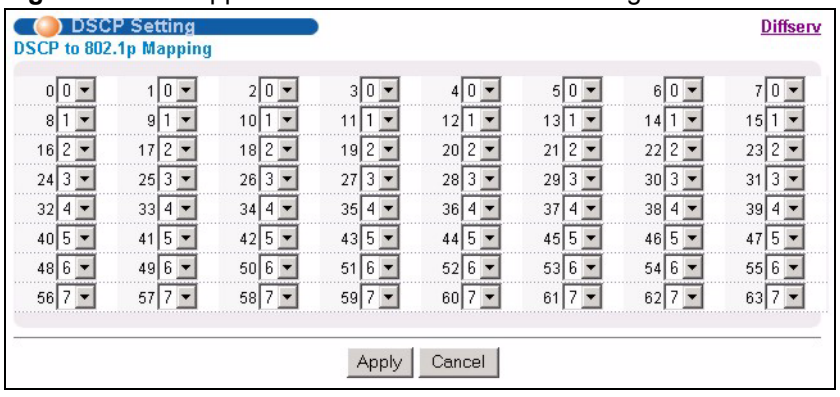
Table 99 Default DSCP-IEEE 802.1p Mapping

DSCP VALUE	0 – 7	8 – 15	16 – 23	24 – 31	32 – 39	40 – 47	48 – 55	56 – 63
IEEE 802.1p	0	1	2	3	4	5	6	7

31.4.1 Configuring DSCP Settings

To change the DSCP-IEEE 802.1p mapping, click the **DSCP Setting** link in the **DiffServ** screen to display the screen as shown next.

Figure 143 IP Application > DiffServ > DSCP Setting



The following table describes the labels in this screen.

Table 100 IP Application > DiffServ > DSCP Setting

LABEL	DESCRIPTION
0 … 63	This is the DSCP classification identification number. To set the IEEE 802.1p priority mapping, select the priority level from the drop-down list box.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

32 DHCP

This chapter shows you how to configure the DHCP feature.

32.1 DHCP Overview

DHCP (Dynamic Host Configuration Protocol RFC 2131 and RFC 2132) allows individual computers to obtain TCP/IP configuration at start-up from a server. You can configure the Switch as a DHCP server or a DHCP relay agent. When configured as a server, the Switch provides the TCP/IP configuration for the clients. If you configure the Switch as a relay agent, then the Switch forwards DHCP requests to DHCP server on your network. If you don't configure the Switch as a DHCP server or relay agent then you must have a DHCP server in the broadcast domain of the client computers or else the client computers must be configured manually.

32.1.1 DHCP Modes

The Switch can be configured as a DHCP server or DHCP relay agent.

- If you configure the Switch as a DHCP server, it will maintain the pool of IP addresses along with subnet masks, DNS server and default gateway information and distribute them to your LAN computers.
- If there is already a DHCP server on your network, then you can configure the Switch as a DHCP relay agent. When the Switch receives a request from a computer on your network, it contacts the DHCP server for the necessary IP information, and then relays the assigned information back to the computer.

32.1.2 DHCP Configuration Options

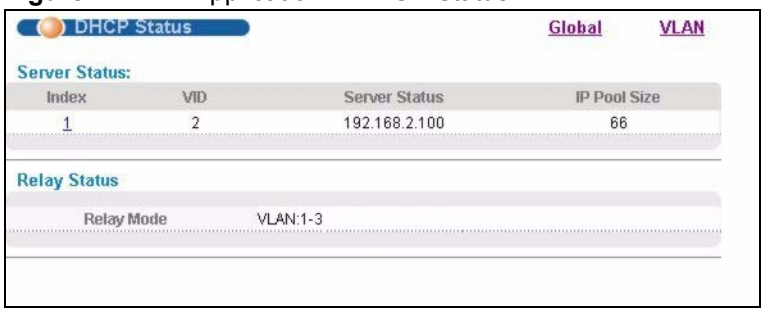
The DHCP configuration on the Switch is divided into **Global** and **VLAN** screens. The screen you should use for configuration depends on the DHCP services you want to offer the DHCP clients on your network. Choose the configuration screen based on the following criteria:

- **Global** - The Switch forwards all DHCP requests to the same DHCP server.
- **VLAN** - The Switch is configured on a VLAN by VLAN basis. The Switch can be configured as a DHCP server for one VLAN and at the same time the Switch can be configured to relay DHCP requests for clients in another VLAN.

32.2 DHCP Status

Click **IP Application** > **DHCP** in the navigation panel. The **DHCP Status** screen displays.

Figure 144 IP Application > DHCP Status



The following table describes the labels in this screen.

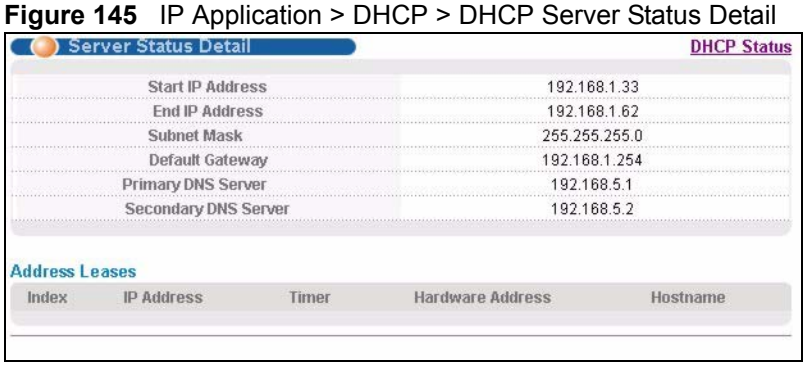
Table 101 IP Application > DHCP Status

LABEL	DESCRIPTION
Server Status	This section displays configuration settings related to the Switch's DHCP server mode.
Index	This is the index number.
VID	This field displays the VLAN ID for which the Switch is a DHCP server.
Server Status	This field displays the starting DHCP client IP address.
IP Pool Size	This field displays the number of IP addresses that can be assigned to clients.
Relay Status	This section displays configuration settings related to the Switch's DHCP relay mode.
Relay Mode	This field displays: • **None** - if the Switch is not configured as a DHCP relay agent. • **Global** - if the Switch is configured as a DHCP relay agent only. • **VLAN** - followed by a VLAN ID if it is configured as a relay agent for specific VLAN(s).

32.3 DHCP Server Status Detail

Click **IP Application** > **DHCP** in the navigation panel and then click an existing index number of a DHCP server configuration to view the screen as shown. Use this screen to view details regarding DHCP server settings configured on the Switch.

Figure 145 IP Application > DHCP > DHCP Server Status Detail



The following table describes the labels in this screen.

Table 102 IP Application > DHCP Server Status Detail

LABEL	DESCRIPTION
Start IP Address	This field displays the starting IP address of the IP address pool configured for this DHCP server instance.
End IP Address	This field displays the last IP address of the IP address pool configured for this DHCP server instance.
Subnet Mask	This field displays the subnet mask value sent to clients from this DHCP server instance.
Default Gateway	This field displays the default gateway value sent to clients from this DHCP server instance.
Primary DNS Server	This field displays the primary DNS server value sent to clients from this DHCP server instance.
Secondary DNS Server	This field displays the secondary DNS server value sent to clients from this DHCP server instance.
Address Leases	This section displays information about the IP addresses this DHCP server issued to clients.
Index	This field displays a sequential number for each DHCP request handled by the Switch.
IP Address	This is the IP address issued to a DHCP client.
Timer	This field displays the time remaining before the DHCP client has to renew its IP address.
Hardware Address	This field displays the MAC address of the DHCP client. It may also display **SELF OCCUPIED ADDRESS** if the IP address cannot be used for DHCP because it is already assigned to the Switch itself.
Hostname	This field displays the system name of the client.

32.4 DHCP Relay

Configure DHCP relay on the Switch if the DHCP clients and the DHCP server are not in the same broadcast domain. During the initial IP address leasing, the Switch helps to relay network information (such as the IP address and subnet mask) between a DHCP client and a DHCP server. Once the DHCP client obtains an IP address and can connect to the network, network information renewal is done between the DHCP client and the DHCP server without the help of the Switch.

The Switch can be configured as a global DHCP relay. This means that the Switch forwards all DHCP requests from all domains to the same DHCP server. You can also configure the Switch to relay DHCP information based on the VLAN membership of the DHCP clients.

32.4.1 DHCP Relay Agent Information

The Switch can add information about the source of client DHCP requests that it relays to a DHCP server by adding **Relay Agent Information**. This helps provide authentication about the source of the requests. The DHCP server can then provide an IP address based on this information. Please refer to RFC 3046 for more details.

The DHCP **Relay Agent Information** feature adds an Agent Information field to the **Option 82** field. The **Option 82** field is in the DHCP headers of client DHCP request frames that the Switch relays to a DHCP server.

Relay Agent Information can include the **System Name** of the Switch if you select this option. You can change the **System Name** in **Basic Settings** > **General Setup**.

The following describes the DHCP relay information that the Switch sends to the DHCP server:

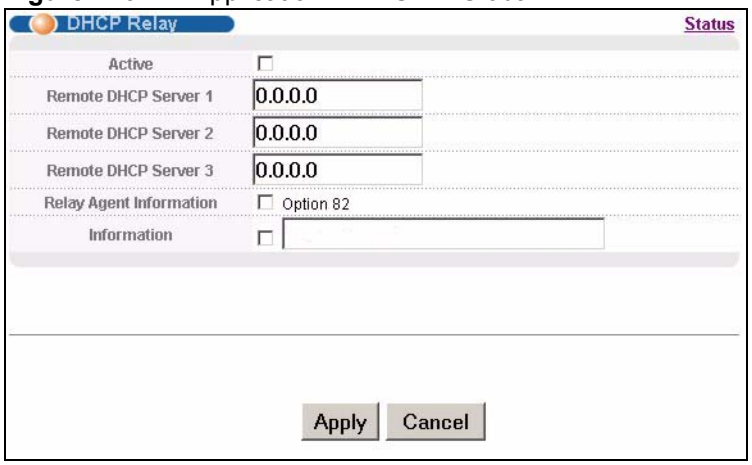
Table 103 Relay Agent Information

FIELD LABELS	DESCRIPTION
Slot ID	(1 byte) This value is always 0 for stand-alone switches.
Port ID	(1 byte) This is the port that the DHCP client is connected to.
VLAN ID	(2 bytes) This is the VLAN that the port belongs to.
Information	(up to 64 bytes) This optional, read-only field is set according to system name set in **Basic Settings > General Setup.**

32.4.2 Configuring DHCP Global Relay

Configure global DHCP relay in the **DHCP Relay** screen. Click **IP Application > DHCP** in the navigation panel and click the **Global** link to display the screen as shown.

Figure 146 IP Application > DHCP > Global



The following table describes the labels in this screen.

Table 104 IP Application > DHCP > Global

LABEL	DESCRIPTION
Active	Select this check box to enable DHCP relay.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
Relay Agent Information	Select the **Option 82** check box to have the Switch add information (slot number, port number and VLAN ID) to client DHCP requests that it relays to a DHCP server.
Information	This read-only field displays the system name you configure in the **General Setup** screen. Select the check box for the Switch to add the system name to the client DHCP requests that it relays to a DHCP server.

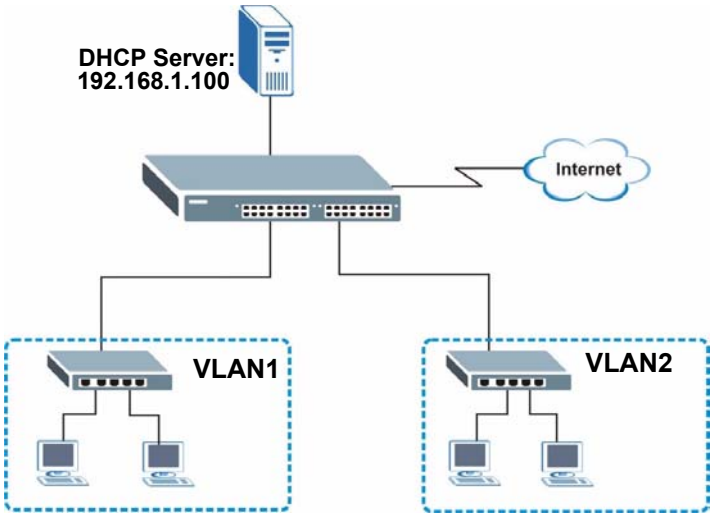
Table 104 IP Application > DHCP > Global (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

32.4.3 Global DHCP Relay Configuration Example

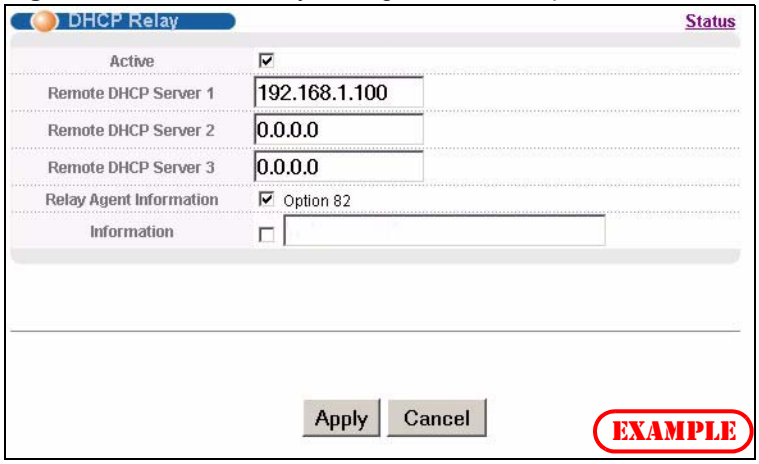
The follow figure shows a network example where the Switch is used to relay DHCP requests for the **VLAN1** and **VLAN2** domains. There is only one DHCP server that services the DHCP clients in both domains.

Figure 147 Global DHCP Relay Network Example



Configure the **DHCP Relay** screen as shown. Make sure you select the **Option 82** check box to set the Switch to send additional information (such as the VLAN ID) together with the DHCP requests to the DHCP server. This allows the DHCP server to assign the appropriate IP address according to the VLAN ID.

Figure 148 DHCP Relay Configuration Example

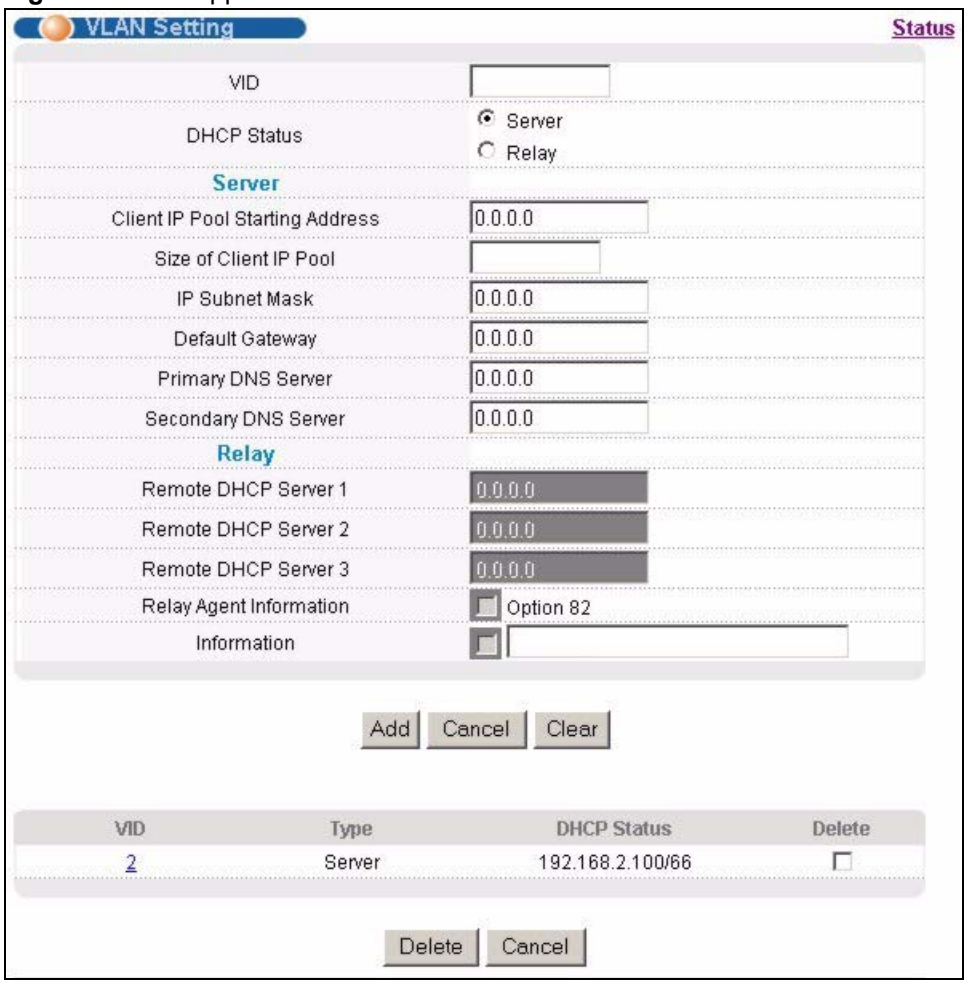


32.5 Configuring DHCP VLAN Settings

Use this screen to configure your DHCP settings based on the VLAN domain of the DHCP clients. Click **IP Application** > **DHCP** in the navigation panel, then click the **VLAN** link In the **DHCP Status** screen that displays.

You must set up a management IP address for each VLAN that you want to configure DHCP settings for on the Switch. See Section 7.6 on page 79 for information on how to do this.

Figure 149 IP Application > DHCP > VLAN



The following table describes the labels in this screen.

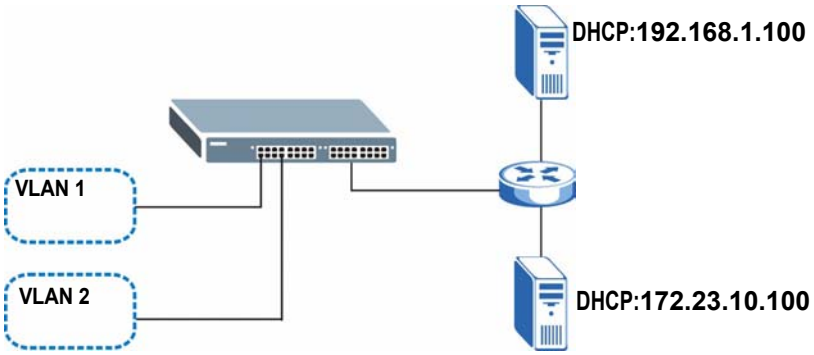
Table 105 IP Application > DHCP > VLAN

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN to which these DHCP settings apply.
DHCP Status	Select whether the Switch should function as a DHCP **Server** or **Relay** for the specified VID. If you select **Server** then fields related to DHCP relay configuration are grayed out and vice versa.
Server	Use this section if you want to configure the Switch to function as a DHCP server for this VLAN.
Client IP Pool Starting Address	Specify the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	Specify the size, or count of the IP address pool. The Switch can issue from 1 to 253 IP addresses to DHCP clients.
IP Subnet Mask	Enter the subnet mask for the client IP pool.
Default Gateway	Enter the IP address of the default gateway device.
Primary/ Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Relay	Use this section if you want to configure the Switch to function as a DHCP relay for this VLAN.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
Relay Agent Information	Select the **Option 82** check box to have the Switch add information (slot number, port number and VLAN ID) to client DHCP requests that it relays to a DHCP server.
Information	This read-only field displays the system name you configure in the **General Setup** screen. Select the check box for the Switch to add the system name to the client DHCP requests that it relays to a DHCP server.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click this to clear the fields above.
VID	This field displays the ID number of the VLAN group to which this DHCP settings apply.
Type	This field displays **Server** or **Relay** for the DHCP mode.
DHCP Status	For DHCP server configuration, this field displays the starting IP address and the size of the IP address pool. For DHCP relay configuration, this field displays the first remote DHCP server IP address.
Delete	Select the configuration entries you want to remove and click **Delete** to remove them.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

32.5.1 Example: DHCP Relay for Two VLANs

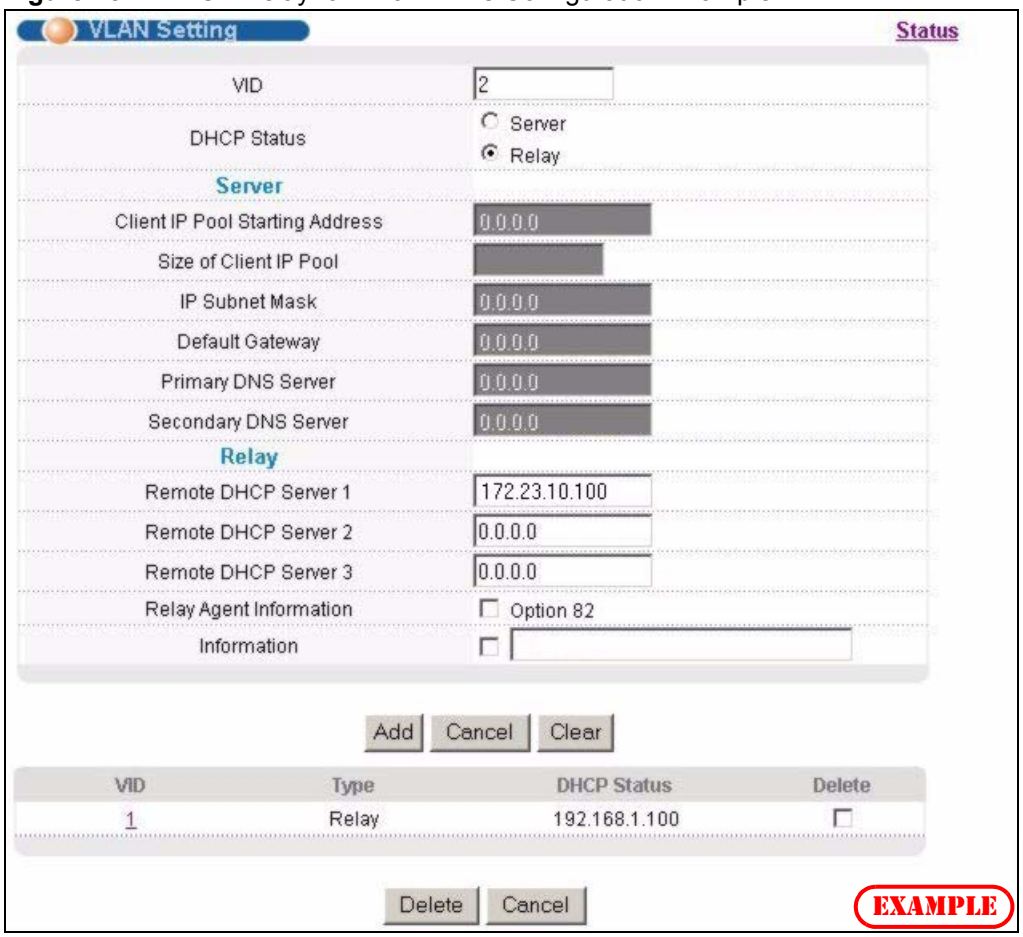
The following example displays two VLANs (VIDs 1 and 2) for a campus network. Two DHCP servers are installed to serve each VLAN. The system is set up to forward DHCP requests from the dormitory rooms (VLAN 1) to the DHCP server with an IP address of 192.168.1.100. Requests from the academic buildings (VLAN 2) are sent to the other DHCP server with an IP address of 172.23.10.100.

Figure 150 DHCP Relay for Two VLANs



For the example network, configure the **VLAN Setting** screen as shown.

Figure 151 DHCP Relay for Two VLANs Configuration Example



33 VRRP

This chapter shows you how to configure and monitor the Virtual Router Redundancy Protocol (VRRP) on the Switch.

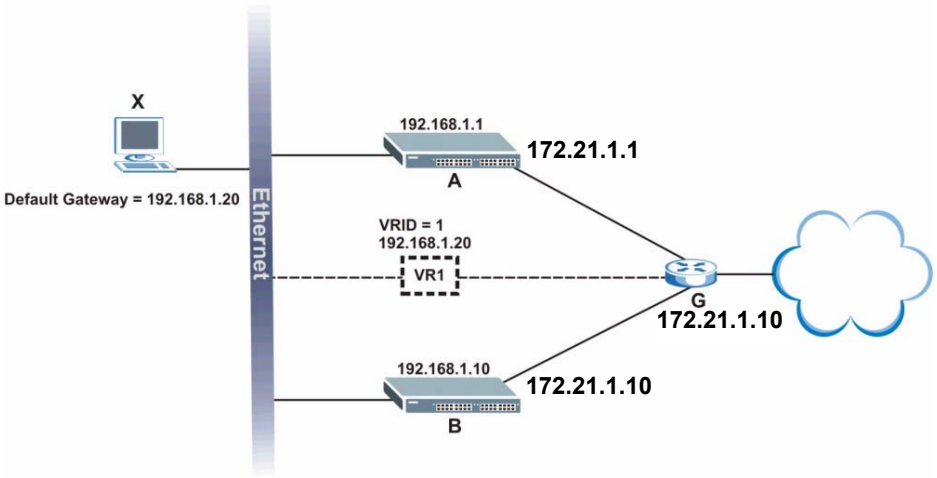
33.1 VRRP Overview

Each host on a network is configured to send packets to a statically configured default gateway (this Switch). The default gateway can become a single point of failure. Virtual Router Redundancy Protocol (VRRP), defined in RFC 2338, allows you to create redundant backup gateways to ensure that the default gateway of a host is always available.

In VRRP, a virtual router (VR) represents a number of physical layer-3 devices. An IP address is associated with the virtual router. A layer-3 device having the same IP address is the preferred master router while the other Layer-3 devices are the backup routers. The master router forwards traffic for the virtual router. When the master router becomes unavailable, a backup router assumes the role of the master router until the master router comes back up and takes over.

The following figure shows a VRRP network example with the switches (**A** and **B**) implementing one virtual router **VR1** to ensure the link between the host **X** and the uplink gateway **G**. Host **X** is configured to use **VR1** (192.168.1.20) as the default gateway. If switch **A** has a higher priority, it is the master router. Switch **B**, having a lower priority, is the backup router.

Figure 152 VRRP: Example 1

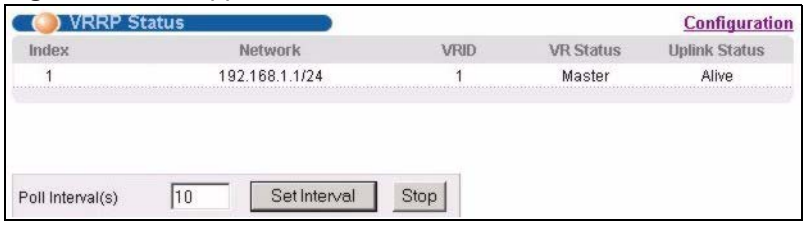


If switch **A** (the master router) is unavailable, switch **B** takes over. Traffic is then processed by switch **B**.

33.2 VRRP Status

Click **IP Application** > **VRRP** in the navigation panel to display the **VRRP Status** screen as shown next.

Figure 153 IP Application > VRRP Status



The following table describes the labels in this screen.

Table 106 IP Application > VRRP Status

LABEL	DESCRIPTION
Index	This field displays the index number of a rule.
Network	This field displays the IP address and the subnet mask bits of an IP routing domain that is associated to a virtual router.
VRID	This field displays the ID number of the virtual router.
VR Status	This field displays the status of the virtual router. This field is **Master** indicating that this Switch functions as the master router. This field is **Backup** indicating that this Switch functions as a backup router. This field displays **Init** when this Switch is initiating the VRRP protocol or when the **Uplink Status** field displays **Dead**.
Uplink Status	This field displays the status of the link between this Switch and the uplink gateway. This field is **Alive** indicating that the link between this Switch and the uplink gateway is up. Otherwise, this field is **Dead**. This field displays **Probe** when this Switch is check for the link state.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt system statistic polling.

33.3 VRRP Configuration

The following sections describe the different parts of the VRRP Configuration screen.

33.3.1 IP Interface Setup

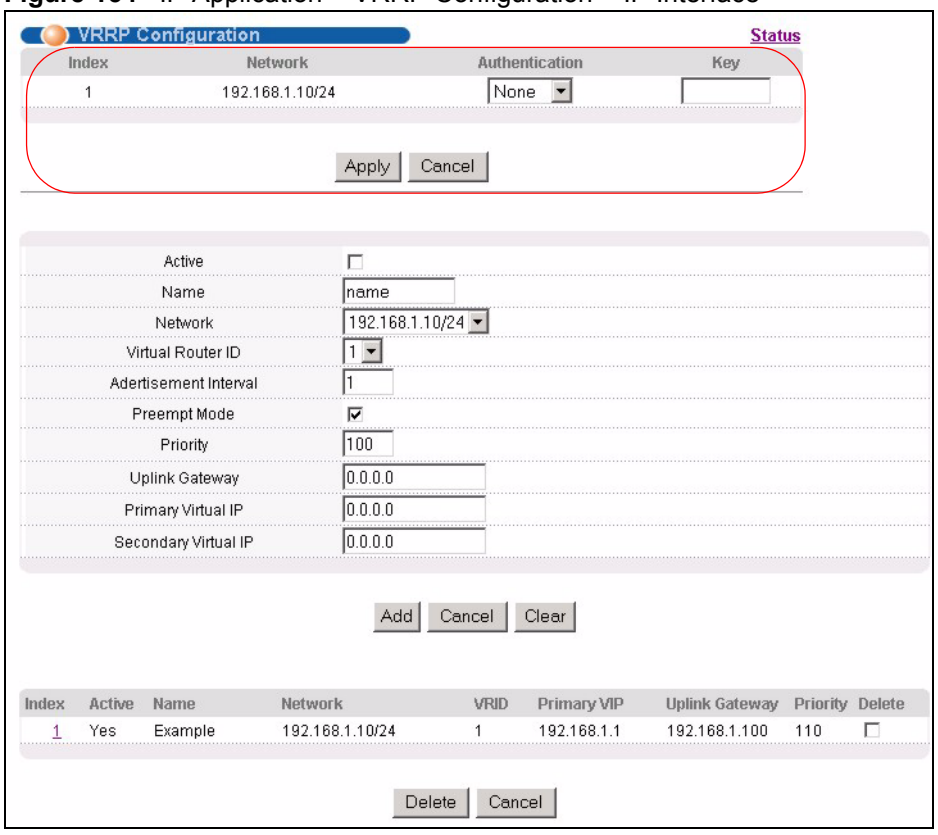
Before configuring VRRP, first create an IP interface (or routing domain) in the **IP Setup** screen (see the Section 7.6 on page 79 for more information).

Click **IP Application**, **VRRP** and click the **Configuration** link to display the **VRRP Configuration** screen as shown next.

You can only configure VRRP on interfaces with unique VLAN IDs.

Routing domains with the same VLAN ID are not displayed in the table indicated.

Figure 154 IP Application > VRRP Configuration > IP Interface



The following table describes the labels in this screen.

Table 107 IP Application > VRRP Configuration > IP Interface

LABEL	DESCRIPTION
Index	This field displays the index number of an entry.
Network	This field displays the IP address and number of subnet mask bit of an IP domain.
Authentication	Select **None** to disable authentication. This is the default setting. Select **Simple** to use a simple password to authenticate VRRP packet exchanges on this interface.

Table 107 IP Application > VRRP Configuration > IP Interface (continued)

LABEL	DESCRIPTION
Key	When you select **Simple** in the **Authentication** field, enter a password key (up to eight printable ASCII character long) in this field.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to discard all changes made in this table.

33.3.2 VRRP Parameters

This section describes the VRRP parameters.

33.3.2.1 Advertisement Interval

The master router sends out Hello messages to let the other backup routers know that it is still up and running. The time interval between sending the Hello messages is the advertisement interval. By default, a Hello message is sent out every second.

If the backup routers do not receive a Hello message from the master router after this interval expires, it is assumed that the master router is down. Then the backup router with the highest priority becomes the master router.

All routers participating in the virtual router must use the same advertisement interval.

33.3.2.2 Priority

Configure the priority level (1 to 254) to set which backup router to take over in case the master router goes down. The backup router with the highest priority will take over. The priority of the VRRP router that owns the IP address(es) associated with the virtual router is 255.

33.3.2.3 Preempt Mode

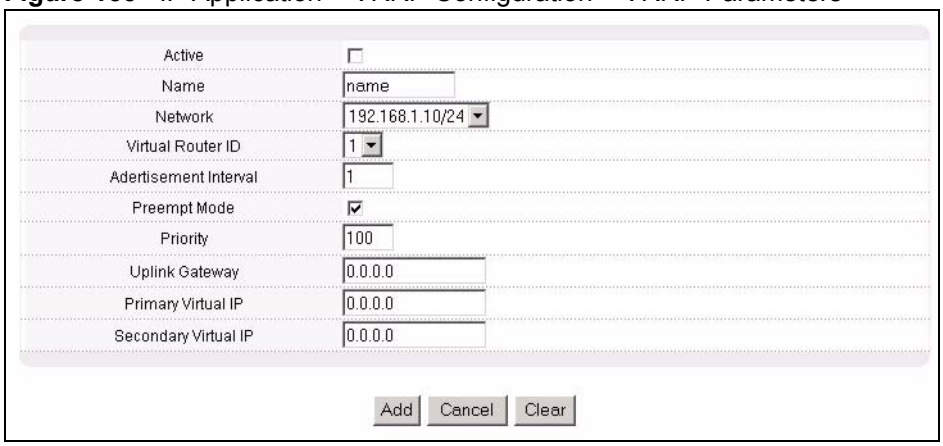
If the master router is unavailable, a backup router assumes the role of the master router. However, when another backup router with a higher priority joins the network, it will preempt the lower priority backup router that is the master. Disable preempt mode to prevent this from happening.

By default, a layer 3 device with the same IP address as the virtual router will become the master router regardless of the preempt mode.

33.3.3 Configuring VRRP Parameters

After you set up an IP interface, configure the VRRP parameters in the **VRRP Configuration** screen.

Figure 155 IP Application > VRRP Configuration > VRRP Parameters



The following table describes the labels in this screen.

Table 108 IP Application > VRRP Configuration > VRRP Parameters

LABEL	DESCRIPTION
Active	Select this option to enable this VRRP entry.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Network	Select an IP domain to which this VRRP entry applies.
Virtual Router ID	Select a virtual router number (1 to 7) for which this VRRP entry is created. You can configure up to seven virtual routers for one network.
Advertisement Interval	Specify the number of seconds between Hello message transmissions. The default is **1**.
Preempt Mode	Select this option to activate preempt mode.
Priority	Enter a number (between 1 and 254) to set the priority level. The bigger the number, the higher the priority. This field is **100** by default.
Uplink Gateway	Enter the IP address of the uplink gateway in dotted decimal notation. The Switch checks the link to the uplink gateway.
Primary Virtual IP	Enter the IP address of the primary virtual router in dotted decimal notation.
Secondary Virtual IP	This field is optional. Enter the IP address of a secondary virtual router in dotted decimal notation. This field is ignored when you enter **0.0.0.0**.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to discard all changes made in this table.
Clear	Click **Clear** to set the above fields back to the factory defaults.

33.3.4 Configuring VRRP Parameters

View the VRRP configuration summary at the bottom of the screen.

Figure 156 VRRP Configuration: Summary

The following table describes the labels in this screen.

Table 109 VRRP Configuring: VRRP Parameters

LABEL	DESCRIPTION
Index	This field displays the index number of an entry.
Active	This field shows whether a VRRP entry is enabled (**Yes**) or disabled (**No**).
Name	This field displays a descriptive name of an entry.
Network	This field displays the IP address and subnet mask of an interface.
VRID	This field displays the ID number of a virtual router.
Primary VIP	This field displays the IP address of the primary virtual router.
Uplink Gateway	This field displays the IP address of the uplink gateway.
Priority	This field displays the priority level (1 to 255) of the entry.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

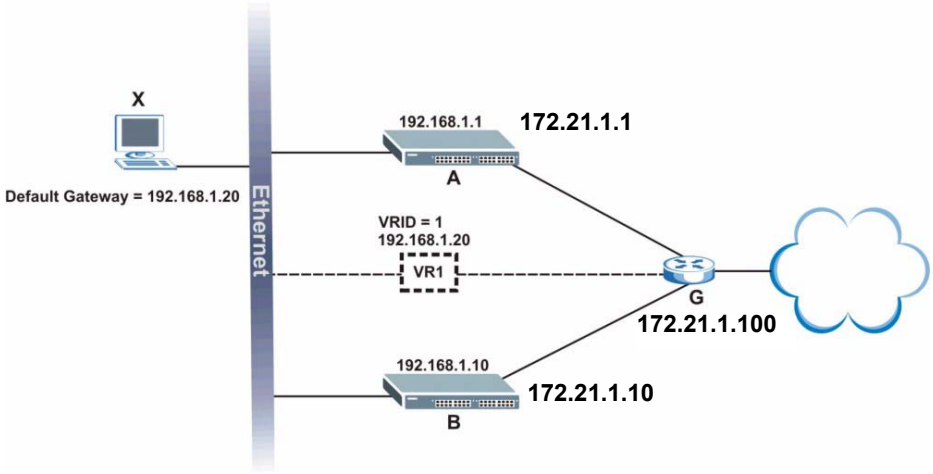
33.4 VRRP Configuration Examples

The following sections show two VRRP configuration examples on the Switch.

33.4.1 One Subnet Network Example

The figure below shows a simple VRRP network with only one virtual router **VR1** (VRID =1) and two switches. The network is connected to the WAN via an uplink gateway **G** (172.21.1.100). The host computer **X** is set to use **VR1** as the default gateway.

Figure 157 VRRP Configuration Example: One Virtual Router Network



You want to set switch **A** as the master router. Configure the VRRP parameters in the **VRRP Configuration** screens on the switches as shown in the figures below.

Figure 158 VRRP Example 1: VRRP Parameter Settings on Switch A

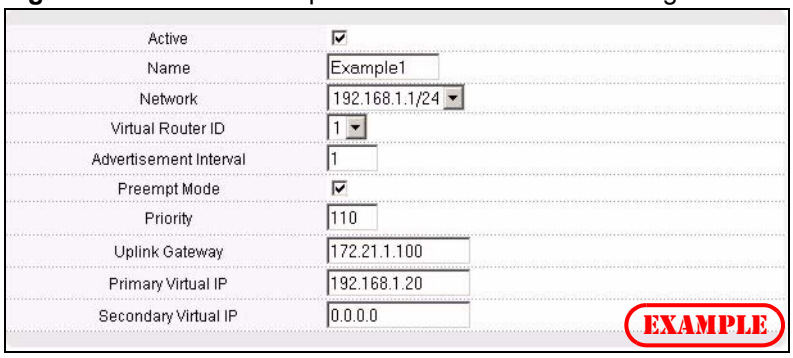
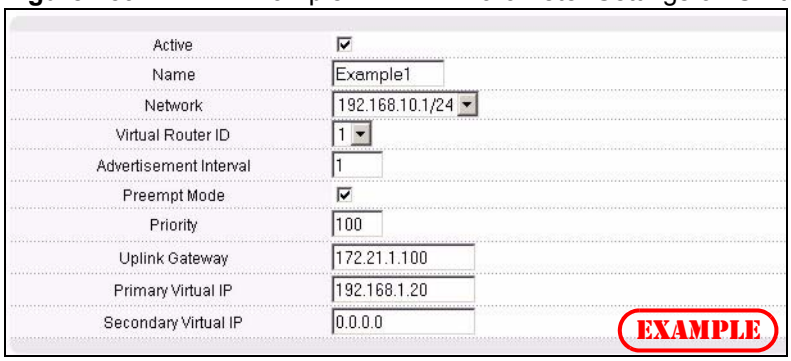


Figure 159 VRRP Example 1: VRRP Parameter Settings on Switch B



After configuring and saving the VRRP configuration, the **VRRP Status** screens for both switches are shown next.

Figure 160 VRRP Example 1: VRRP Status on Switch A

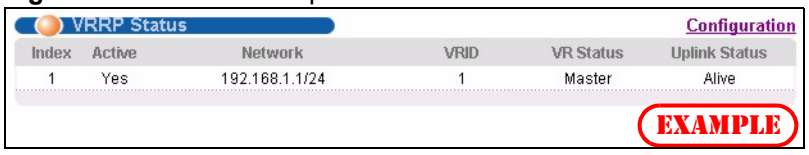
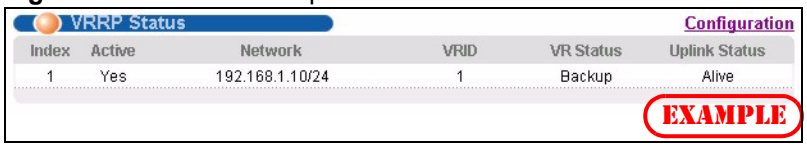


Figure 161 VRRP Example 1: VRRP Status on Switch B

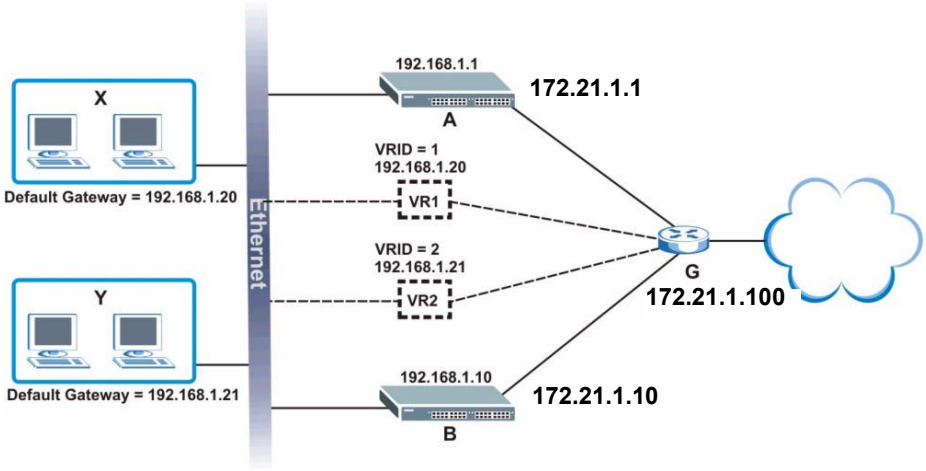


33.4.2 Two Subnets Example

The following figure depicts an example in which two switches share the network traffic. Hosts in the two network groups use different default gateways. Each switch is configured to backup a virtual router using VRRP.

You wish to configure switch **A** as the master router for virtual router **VR1** and as a backup for virtual router **VR2**. On the other hand, switch **B** is the master for **VR2** and a backup for **VR1**.

Figure 162 VRRP Configuration Example: Two Virtual Router Network



You need to configure the **VRRP Configuration** screen for virtual router VR2 on each switch, while keeping the VRRP configuration in example 1 for virtual router **VR1** (refer to Section 33.4.2 on page 273). Configure the VRRP parameters on the switches as shown in the figures below.

Figure 163 VRRP Example 2: VRRP Parameter Settings for VR2 on Switch A

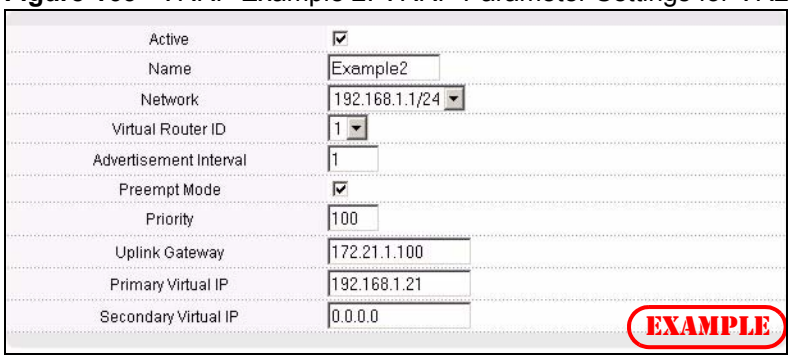
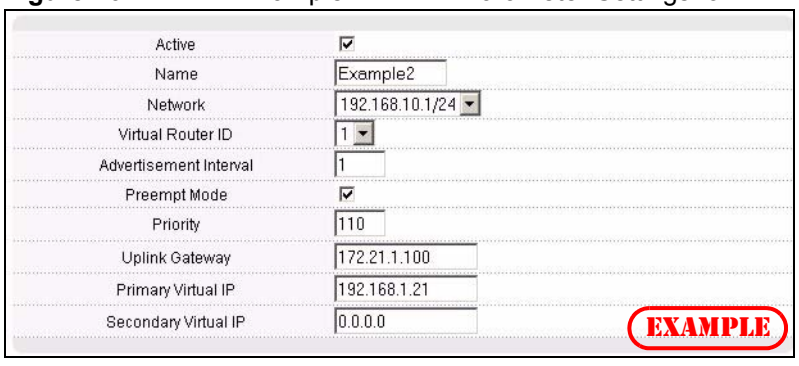
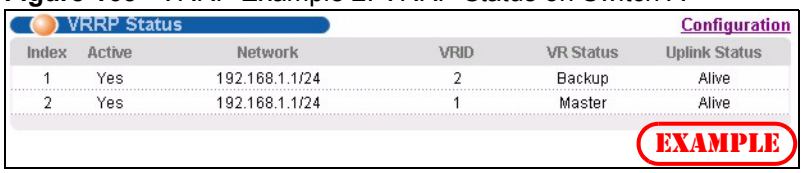


Figure 164 VRRP Example 2: VRRP Parameter Settings for VR2 on Switch B



After configuring and saving the VRRP configuration, the **VRRP Status** screens for both switches are shown next.

Figure 165 VRRP Example 2: VRRP Status on Switch A

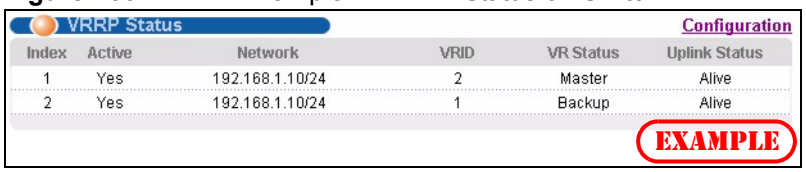

VRRP Status

Configuration

Index	Active	Network	VRID	VR Status	Uplink Status
1	Yes	192.168.1.1/24	2	Backup	Alive
2	Yes	192.168.1.1/24	1	Master	Alive

EXAMPLE

Figure 166 VRRP Example 2: VRRP Status on Switch B


VRRP Status

Configuration

Index	Active	Network	VRID	VR Status	Uplink Status
1	Yes	192.168.1.10/24	2	Master	Alive
2	Yes	192.168.1.10/24	1	Backup	Alive

EXAMPLE

PART V
Management

Maintenance (279)
Access Control (285)
Diagnostic (303)
Syslog (305)
Cluster Management (309)
MAC Table (315)
IP Table (317)
ARP Table (319)
Routing Table (321)
Configure Clone (323)

34

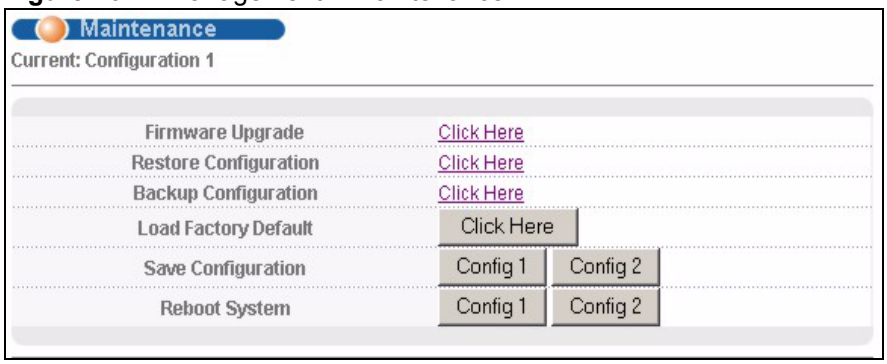
Maintenance

This chapter explains how to configure the maintenance screens that let you maintain the firmware and configuration files.

34.1 The Maintenance Screen

Use this screen to manage firmware and your configuration files. Click **Management** > **Maintenance** in the navigation panel to open the following screen.

Figure 167 Management > Maintenance



The following table describes the labels in this screen.

Table 110 Management > Maintenance

LABEL	DESCRIPTION
Current	This field displays which configuration (**Configuration 1** or **Configuration 2**) is currently operating on the Switch.
Firmware Upgrade	Click **Click Here** to go to the **Firmware Upgrade** screen.
Restore Configuration	Click **Click Here** to go to the **Restore Configuration** screen.
Backup Configuration	Click **Click Here** to go to the **Backup Configuration** screen.
Load Factory Default	Click **Click Here** to reset the configuration to the factory default settings.

Table 110 Management > Maintenance (continued)

LABEL	DESCRIPTION
Save Configuration	Click **Config 1** to save the current configuration settings to **Configuration 1** on the Switch. Click **Config 2** to save the current configuration settings to **Configuration 2** on the Switch.
Reboot System	Click **Config 1** to reboot the system and load **Configuration 1** on the Switch. Click **Config 2** to reboot the system and load **Configuration 2** on the Switch. Note: Make sure to click the **Save** button in any screen to save your settings to the current configuration on the Switch.

34.2 Load Factory Default

Follow the steps below to reset the Switch back to the factory defaults.

1. In the **Maintenance** screen, click the **Click Here** button next to **Load Factory Default** to clear all Switch configuration information you configured and return to the factory defaults.
2. Click **OK** to reset all Switch configurations to the factory defaults.

Figure 168 Load Factory Default: Start

3. In the web configurator, click the **Save** button to make the changes take effect. If you want to access the Switch web configurator again, you may need to change the IP address of your computer to be in the same subnet as that of the default Switch IP address (192.168.1.1).

34.3 Save Configuration

Click **Config 1** to save the current configuration settings permanently to **Configuration 1** on the Switch.

Click **Config 2** to save the current configuration settings to **Configuration 2** on the Switch.

Alternatively, click **Save** on the top right-hand corner in any screen to save the configuration changes to the current configuration.

Clicking the **Apply** or **Add** button does NOT save the changes permanently. All unsaved changes are erased after you reboot the Switch.

34.4 Reboot System

Reboot System allows you to restart the Switch without physically turning the power off. It also allows you to load configuration one (**Config 1**) or configuration two (**Config 2**) when you reboot. Follow the steps below to reboot the Switch.

1. In the **Maintenance** screen, click the **Config 1** button next to **Reboot System** to reboot and load configuration one. The following screen displays.

Figure 169 Reboot System: Confirmation

2. Click **OK** again and then wait for the Switch to restart. This takes up to two minutes. This does not affect the Switch's configuration.

Click **Config 2** and follow steps 1 to 2 to reboot and load configuration two on the Switch.

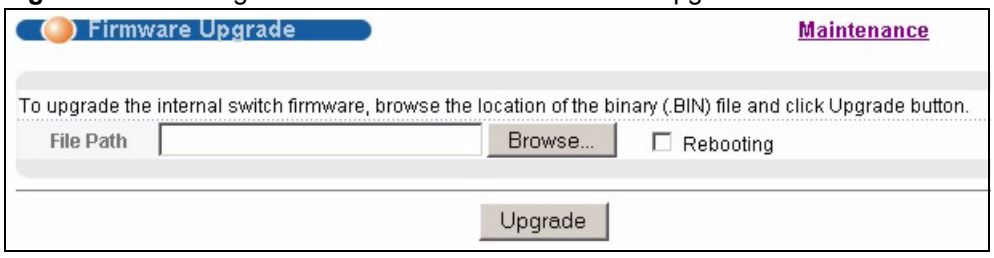
34.5 Firmware Upgrade

Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

From the **Maintenance** screen, display the **Firmware Upgrade** screen as shown next.

Figure 170 Management > Maintenance > Firmware Upgrade



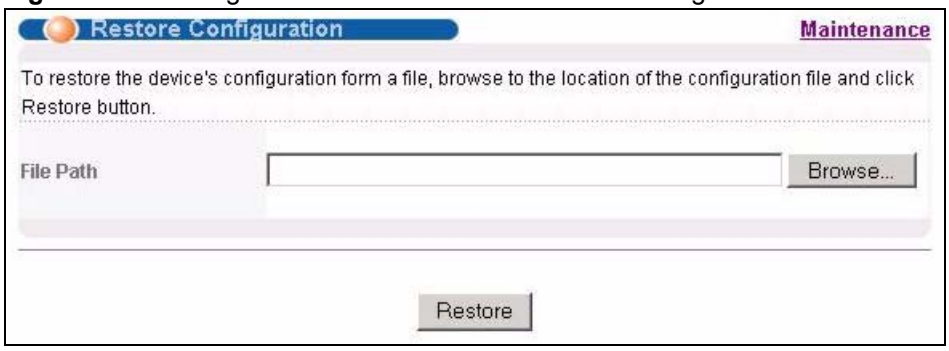
Type the path and file name of the firmware file you wish to upload to the Switch in the **File Path** text box or click **Browse** to locate it. Select the **Rebooting** checkbox if you want to reboot the Switch and apply the new firmware immediately. (Firmware upgrades are only applied after a reboot). Click **Upgrade** to load the new firmware.

After the firmware upgrade process is complete, see the **System Info** screen to verify your current firmware version number.

34.6 Restore a Configuration File

Restore a previously saved configuration from your computer to the Switch using the **Restore Configuration** screen.

Figure 171 Management > Maintenance > Restore Configuration


Restore Configuration
Maintenance
To restore the device's configuration form a file, browse to the location of the configuration file and click Restore button.
File Path
Browse...
Restore

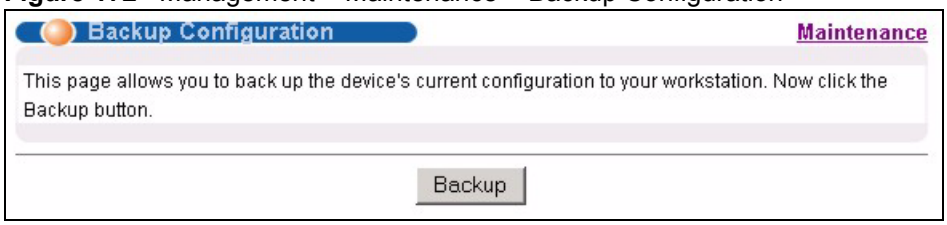
Type the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Browse** to display the **Choose File** screen from which you can locate it. After you have specified the file, click **Restore**. "config" is the name of the configuration file on the Switch, so your backup configuration file is automatically renamed when you restore using this screen.

34.7 Backup a Configuration File

Backing up your Switch configurations allows you to create various “snapshots” of your device from which you may restore at a later date.

Back up your current Switch configuration to a computer using the **Backup Configuration** screen.

Figure 172 Management > Maintenance > Backup Configuration


Backup Configuration
Maintenance
This page allows you to back up the device's current configuration to your workstation. Now click the Backup button.
Backup

Follow the steps below to back up the current Switch configuration to your computer in this screen.

1. Click **Backup**.
2. Click **Save** to display the **Save As** screen.
3. Choose a location to save the file on your computer from the **Save in** drop-down list box and type a descriptive name for it in the **File name** list box. Click **Save** to save the configuration file to your computer.

34.8 FTP Command Line

This section shows some examples of uploading to or downloading files from the Switch using FTP commands. First, understand the filename conventions.

34.8.1 Filename Conventions

The configuration file (also known as the romfile or ROM) contains the factory default settings in the screens such as password, Switch setup, IP Setup, and so on. Once you have customized the Switch's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System, sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension.

Table 111 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	config	.cfg	This is the configuration (config) filename on the Switch. Uploading the config file replaces the specified configuration file system, including your Switch configurations, system-related data (including the default password), the error log and the trace log.
Firmware	ras	*.bin	This is the generic name for the ZyNOS firmware on the Switch.

34.8.1.1 Example FTP Commands

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the Switch.

```
ftp> get config config.cfg
```

This is a sample FTP session saving the current configuration to a file called "config.cfg" on your computer.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the Switch only recognizes "config" and "ras". Be sure you keep unaltered copies of both files for later use.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

34.8.2 FTP Command Line Procedure

1. Launch the FTP client on your computer.
2. Enter `open`, followed by a space and the IP address of your Switch.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is "1234").

5 Enter `bin` to set transfer mode to binary.
6 Use `put` to transfer files from the computer to the Switch, for example, `put firmware.bin ras` transfers the firmware on your computer (firmware.bin) to the Switch and renames it to "ras". Similarly, `put config.cfg config` transfers the configuration file on your computer (config.cfg) to the Switch and renames it to "config". Likewise `get config config.cfg` transfers the configuration file on the Switch to your computer and renames it to "config.cfg". See Table 111 on page 283 for more information on filename conventions.
7 Enter `quit` to exit the ftp prompt.

34.8.3 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 112 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

34.8.4 FTP Restrictions

FTP will not work when:

- FTP service is disabled in the **Service Access Control** screen.
- The IP address(es) in the **Remote Management** screen does not match the client IP address. If it does not match, the Switch will disconnect the FTP session immediately.

35

Access Control

This chapter describes how to control access to the Switch.

35.1 Access Control Overview

A console port and FTP are allowed one session each, Telnet and SSH share nine sessions, up to five Web sessions (five different usernames and passwords) and/or limitless SNMP access control sessions are allowed.

Table 113 Access Control Overview

Console Port	SSH	Telnet	FTP	Web	SNMP
One session	Share up to nine sessions		One session	Up to five accounts	No limit

A console port access control session and Telnet access control session cannot coexist when multi-login is disabled. See Section 44.12.2 on page 341 for more information on disabling multi-login.

35.2 The Access Control Main Screen

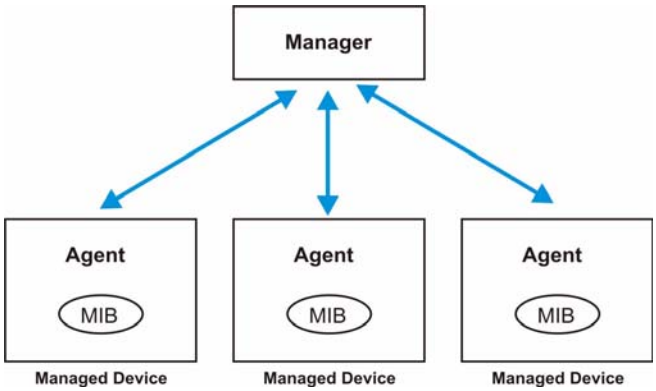
Click **Management** > **Access Control** in the navigation panel to display the main screen as shown.

Figure 173 Management > Access Control

35.3 About SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol used to manage and monitor TCP/IP-based devices. SNMP is used to exchange management information between the network management system (NMS) and a network element (NE). A manager station can manage and monitor the Switch through the network via SNMP version one (SNMPv1), SNMP version 2c or SNMP version 3. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 174 SNMP Management Model



An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed Switch (the Switch). An agent translates the local management information from the managed Switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a Switch. Examples of variables include number of packets received, node port status and so on. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 114 SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

35.3.1 SNMP v3 and Security

SNMP v3 enhances security for SNMP management. SNMP managers can be required to authenticate with agents before conducting SNMP management sessions.

Security can be further enhanced by encrypting the SNMP messages sent from the managers. Encryption protects the contents of the SNMP messages. When the contents of the SNMP messages are encrypted, only the intended recipients can read them.

35.3.2 Supported MIBs

MIBs let administrators collect statistics and monitor status and performance.

The Switch supports the following MIBs:

- SNMP MIB II (RFC 1213)
- RFC 1157 SNMP v1
- RFC 1493 Bridge MIBs
- RFC 1643 Ethernet MIBs
- RFC 1155 SMI
- RFC 2674 SNMPv2, SNMPv2c
- RFC 1757 RMON
- SNMPv2, SNMPv2c or later version, compliant with RFC 2011 SNMPv2 MIB for IP, RFC 2012 SNMPv2 MIB for TCP, RFC 2013 SNMPv2 MIB for UDP

35.3.3 SNMP Traps

The Switch sends traps to an SNMP manager when an event occurs. The following tables outline the SNMP traps by category.

An OID (Object ID) that begins with "**1.3.6.1.4.1.890.1.5.8.**" is defined in private MIBs. Otherwise, it is a standard MIB OID.

Table 115 SNMP System Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
coldstart	coldStart	1.3.6.1.6.3.1.1.5.1	This trap is sent when the Switch is turned on.
warmstart	warmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent when the Switch restarts.
fanspeed	FanSpeedEventOn	1.3.6.1.4.1.890.1.5.8.39.31.2.1	This trap is sent when the fan speed goes above or below the normal operating range.
	FanSpeedEventClear	1.3.6.1.4.1.890.1.5.8.39.31.2.2	This trap is sent when the fan speed returns to the normal operating range.

Table 115 SNMP System Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
temperature	TemperatureEventOn	1.3.6.1.4.1.890.1.5.8.39.31.2.1	This trap is sent when the temperature goes above or below the normal operating range.
	TemperatureEventClear	1.3.6.1.4.1.890.1.5.8.39.31.2.2	This trap is sent when the temperature returns to the normal operating range.
voltage	VoltageEventOn	1.3.6.1.4.1.890.1.5.8.39.31.2.1	This trap is sent when the voltage goes above or below the normal operating range.
	VoltageEventClear	1.3.6.1.4.1.890.1.5.8.39.31.2.2	This trap is sent when the voltage returns to the normal operating range.
reset	UncontrolledResetEventOn	1.3.6.1.4.1.890.1.5.8.39.31.2.1	This trap is sent when the Switch automatically resets.
	ControlledResetEventOn	1.3.6.1.4.1.890.1.5.8.39.31.2.1	This trap is sent when the Switch resets by an administrator through a management interface.
	RebootEvent	1.3.6.1.4.1.890.1.5.1.1.2	This trap is sent when the Switch reboots by an administrator through a management interface.
timesync	RTCNotUpdatedEventOn	1.3.6.1.4.1.890.1.5.8.39.31.2.1	This trap is sent when the Switch fails to get the time and date from a time server.
	RTCNotUpdatedEventClear	1.3.6.1.4.1.890.1.5.8.39.31.2.2	This trap is sent when the Switch gets the time and date from a time server.
intrusionlock	IntrusionLockEventOn	1.3.6.1.4.1.890.1.5.8.39.31.2.1	This trap is sent when intrusion lock occurs on a port.
loopguard	LoopguardEventOn	1.3.6.1.4.1.890.1.5.8.39.31.2.1	This trap is sent when loopguard shuts down a port.

Table 116 SNMP InterfaceTraps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
linkup	linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
	LinkDownEventClear	1.3.6.1.4.1.890.1.5.8.39.31.2.2	This trap is sent when the Ethernet link is up.
linkdown	linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
	LinkDownEventOn	1.3.6.1.4.1.890.1.5.8.39.31.2.1	This trap is sent when the Ethernet link is down.

Table 116 SNMP InterfaceTraps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
autonegotiation	AutonegotiationFailedEventOn	1.3.6.1.4.1.890.1.5.8.39.31.2.1	This trap is sent when an Ethernet interface fails to auto-negotiate with the peer Ethernet interface.
	AutonegotiationFailedEventClear	1.3.6.1.4.1.890.1.5.8.39.31.2.2	This trap is sent when an Ethernet interface auto-negotiates with the peer Ethernet interface.

Table 117 AAA Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
authentication	authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when authentication fails due to incorrect user name and/or password.
	AuthenticationFailureEventOn	1.3.6.1.4.1.890.1.5.8.39.31.2.1	This trap is sent when authentication fails due to incorrect user name and/or password.
	RADIUSNotReachableEventOn	1.3.6.1.4.1.890.1.5.8.39.31.2.1	This trap is sent when there is no response message from the RADIUS server.
	RADIUSNotReachableEventClear	1.3.6.1.4.1.890.1.5.8.39.31.2.2	This trap is sent when the RADIUS server can be reached.
accounting	RADIUSAcctNotReachableEventOn	1.3.6.1.4.1.890.1.5.8.39.31.2.1	This trap is sent when there is no response message from the RADIUS accounting server.
	RADIUSAcctNotReachableEventClear	1.3.6.1.4.1.890.1.5.8.39.31.2.2	This trap is sent when the RADIUS accounting server can be reached.

Table 118 SNMP IP Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
ping	pingProbeFailed	1.3.6.1.2.1.80.0.1	This trap is sent when a single ping probe fails.
	pingTestFailed	1.3.6.1.2.1.80.0.2	This trap is sent when a ping test (consisting of a series of ping probes) fails.
	pingTestCompleted	1.3.6.1.2.1.80.0.3	This trap is sent when a ping test is completed.
traceroute	traceRouteTestFailed	1.3.6.1.2.1.81.0.2	This trap is sent when a traceroute test fails.
	traceRouteTestCompleted	1.3.6.1.2.1.81.0.3	This trap is sent when a traceroute test is completed.

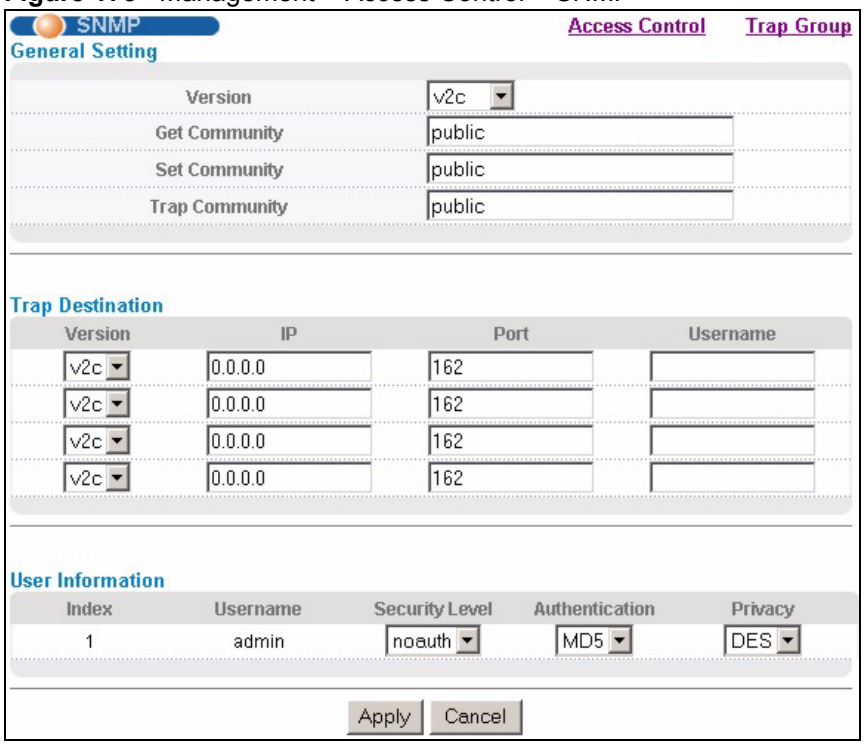
Table 119 SNMP Switch Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
stp	STPNewRoot	1.3.6.1.2.1.17.0.1	This trap is sent when the STP root switch changes.
	MRSTPNewRoot	1.3.6.1.4.1.890.1.5.8.39.43.2.1	This trap is sent when the MRSTP root switch changes.
	MSTPNewRoot	1.3.6.1.4.1.890.1.5.8.39.107.70.1	This trap is sent when the MSTP root switch changes.
	STPTopologyChange	1.3.6.1.2.1.17.0.2	This trap is sent when the STP topology changes.
	MRSTPTopologyChange	1.3.6.1.4.1.890.1.5.8.39.43.2.2	This trap is sent when the MRSTP topology changes.
	MSTPTopologyChange	1.3.6.1.4.1.890.1.5.8.39.107.70.2	This trap is sent when the MSTP root switch changes.
mactable	MacTableFullEventOn	1.3.6.1.4.1.890.1.5.8.39.31.2.1	This trap is sent when more than 99% of the MAC table is used.
	MacTableFullEventClear	1.3.6.1.4.1.890.1.5.8.39.31.2.2	This trap is sent when less than 95% of the MAC table is used.
rmon	RmonRisingAlarm	1.3.6.1.4.1.890.1.5.1.1.16.0.1	This trap is sent when a variable goes over the RMON "rising" threshold.
	RmonFallingAlarm	1.3.6.1.4.1.890.1.5.1.1.16.0.2	This trap is sent when the variable falls below the RMON "falling" threshold.

35.3.4 Configuring SNMP

From the **Access Control** screen, display the **SNMP** screen. You can click **Access Control** to go back to the **Access Control** screen.

Figure 175 Management > Access Control > SNMP



The following table describes the labels in this screen.

Table 120 Management > Access Control > SNMP

LABEL	DESCRIPTION
General Setting	Use this section to specify the SNMP version and community (password) values.
Version	Select the SNMP version for the Switch. The SNMP version on the Switch must match the version on the SNMP manager. Choose SNMP version 2c (**v2c**), SNMP version 3 (**v3**) or both (**v3v2c**). Note: SNMP version 2c is backwards compatible with SNMP version 1.
Get Community	Enter the **Get Community** string, which is the password for the incoming Get- and GetNext- requests from the management station. The **Get Community** string is only used by SNMP managers using SNMP version 2c or lower.
Set Community	Enter the **Set Community**, which is the password for incoming Set- requests from the management station. The **Set Community** string is only used by SNMP managers using SNMP version 2c or lower.
Trap Community	Enter the **Trap Community** string, which is the password sent with each trap to the SNMP manager. The **Trap Community** string is only used by SNMP managers using SNMP version 2c or lower.
Trap Destination	Use this section to configure where to send SNMP traps from the Switch.
Version	Specify the version of the SNMP trap messages.
IP	Enter the IP addresses of up to four managers to send your SNMP traps to.
Port	Enter the port number upon which the manager listens for SNMP traps.

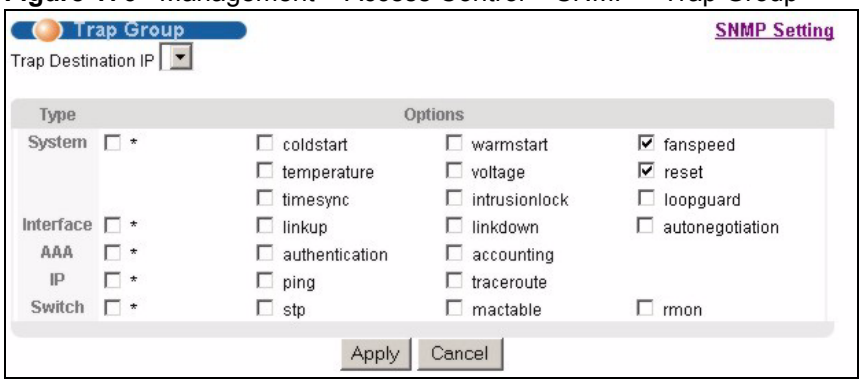
Table 120 Management > Access Control > SNMP (continued)

LABEL	DESCRIPTION
Username	Enter the username to be sent to the SNMP manager along with the SNMP v3 trap. Note: This username must match an existing account on the Switch (configured in **Management > Access Control > Logins** screen).
User Information	Use this section to configure users for authentication with managers using SNMP v3. Note: Use the username and password of the login accounts you specify in this section to create accounts on the SNMP v3 manager.
Index	This is a read-only number identifying a login account on the Switch.
Username	This field displays the username of a login account on the Switch.
Security Level	Select whether you want to implement authentication and/or encryption for SNMP communication from this user. Choose: • **noauth** -to use the username as the password string to send to the SNMP manager. This is equivalent to the Get, Set and Trap Community in SNMP v2c. This is the lowest security level. • **auth** - to implement an authentication algorithm for SNMP messages sent by this user. • **priv** - to implement authentication and encryption for SNMP messages sent by this user. This is the highest security level. Note: The settings on the SNMP manager must be set at the same security level or higher than the security level settings on the Switch.
Authentication	Select an authentication algorithm. MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5, but is slower.
Privacy	Specify the encryption method for SNMP communication from this user. You can choose one of the following: • **DES** - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data. • **AES** - Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

35.3.5 Configuring SNMP Trap Group

From the **SNMP** screen, click **Trap Group** to view the screen as shown. Use the **Trap Group** screen to specify the types of SNMP traps that should be sent to each SNMP manager.

Figure 176 Management > Access Control > SNMP > Trap Group



The following table describes the labels in this screen.

Table 121 Management > Access Control > SNMP > Trap Group

LABEL	DESCRIPTION
Trap Destination IP	Select one of your configured trap destination IP addresses. These are the IP addresses of the SNMP managers. You must first configure a trap destination IP address in the **SNMP Setting** screen. Use the rest of the screen to select which traps the Switch sends to that SNMP manager.
Type	Select the categories of SNMP traps that the Switch is to send to the SNMP manager.
Options	Select the individual SNMP traps that the Switch is to send to the SNMP station. See Section 35.3.3 on page 287 for individual trap descriptions. The traps are grouped by category. Selecting a category automatically selects all of the category's traps. Clear the check boxes for individual traps that you do not want the Switch to send to the SNMP station. Clearing a category's check box automatically clears all of the category's trap check boxes (the Switch only sends traps from selected categories).
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

35.3.6 Setting Up Login Accounts

Up to five people (one administrator and four non-administrators) may access the Switch via web configurator at any one time.

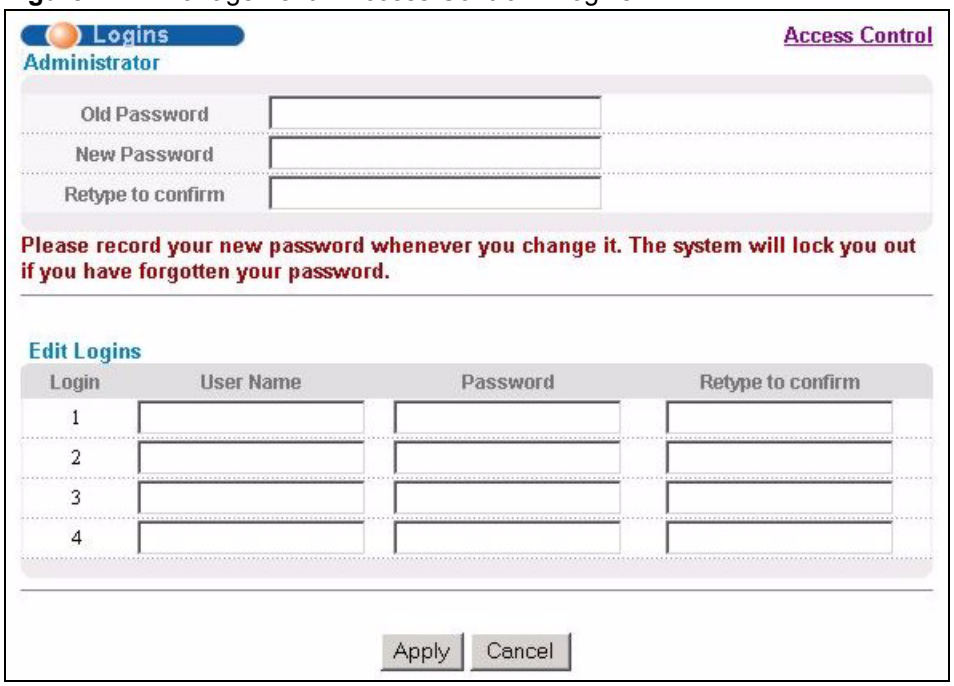
- An administrator is someone who can both view and configure Switch changes. The username for the Administrator is always **admin**. The default administrator password is **1234**.

It is highly recommended that you change the default administrator password (**1234**).

- A non-administrator (username is something other than **admin**) is someone who can view but not configure Switch settings.

Click **Management > Access Control > Logins** to view the screen as shown.

Figure 177 Management > Access Control > Logins



The following table describes the labels in this screen.

Table 122 Management > Access Control > Logins

LABEL	DESCRIPTION
Administrator This is the default administrator account with the “admin” user name. You cannot change the default administrator user name. Only the administrator has read/write access.	
Old Password	Type the existing system password (**1234** is the default password when shipped).
New Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Edit Logins You may configure passwords for up to four users. These users have read-only access. You can give users higher privileges via the CLI. For more information on assigning privileges see Chapter 44 on page 333.	
User Name	Set a user name (up to 32 ASCII characters long).
Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Apply	Click **Apply** to save your changes to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

35.4 SSH Overview

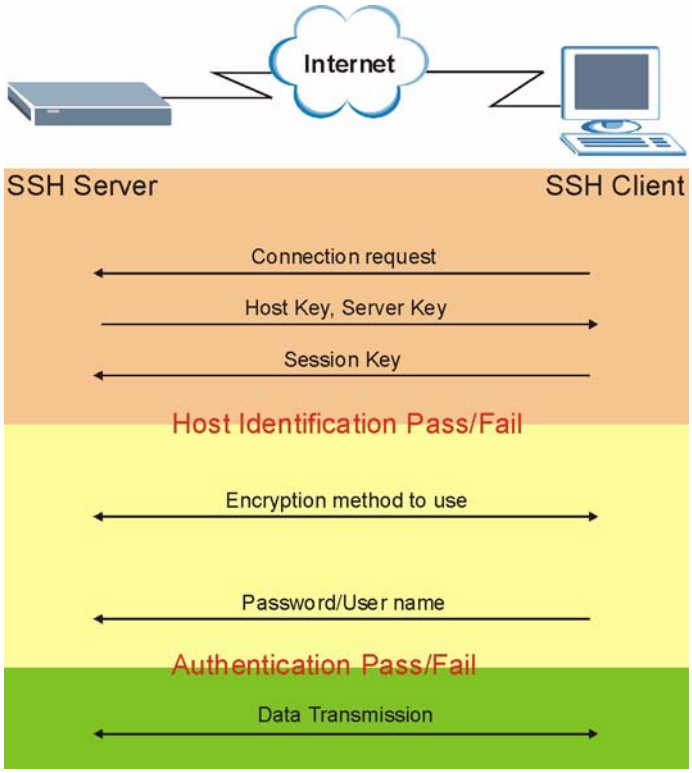
Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

Figure 178 SSH Communication Example

35.5 How SSH works

The following table summarizes how a secure connection is established between two remote hosts.

Figure 179 How SSH Works



1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method
Once the identification is verified, both the client and server must agree on the type of encryption method to use.
3 Authentication and Data Transmission
After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

35.6 SSH Implementation on the Switch

Your Switch supports SSH version 2 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the Switch for remote management and file transfer on port 22. Only one SSH connection is allowed at a time.

35.6.1 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the Switch over SSH.

35.7 Introduction to HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

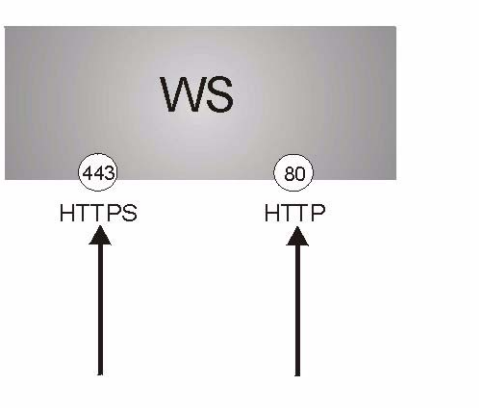
It relies upon certificates, public keys, and private keys.

HTTPS on the Switch is used so that you may securely access the Switch using the web configurator. The SSL protocol specifies that the SSL server (the Switch) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the Switch), whereas the SSL client only should authenticate itself when the SSL server requires it to do so. Authenticating client certificates is optional and if selected means the SSL-client must send the Switch a certificate. You must apply for a certificate for the browser from a Certificate Authority (CA) that is a trusted CA on the Switch.

Please refer to the following figure.

1 HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the Switch's WS (web server).
2 HTTP connection requests from a web browser go to port 80 (by default) on the Switch's WS (web server).

Figure 180 HTTPS Implementation



If you disable **HTTP** in the **Service Access Control** screen, then the Switch blocks all HTTP connection attempts.

35.8 HTTPS Example

If you haven't changed the default HTTPS port on the Switch, then in your browser enter "https://Switch IP Address/" as the web site address where "Switch IP Address" is the IP address or domain name of the Switch you wish to access.

35.8.1 Internet Explorer Warning Messages

When you attempt to access the Switch HTTPS server, a Windows dialog box pops up asking if you trust the server certificate. Click **View Certificate** if you want to verify that the certificate is from the Switch.

You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the web configurator login screen; if you select **No**, then web configurator access is blocked.

Figure 181 Security Alert Dialog Box (Internet Explorer)

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

35.8.2 Netscape Navigator Warning Messages

When you attempt to access the Switch HTTPS server, a **Website Certified by an Unknown Authority** screen pops up asking if you trust the server certificate. Click **Examine Certificate** if you want to verify that the certificate is from the Switch.

If **Accept this certificate temporarily for this session** is selected, then click **OK** to continue in Netscape.

Select **Accept this certificate permanently** to import the Switch's certificate into the SSL client.

Figure 182 Security Certificate 1 (Netscape)

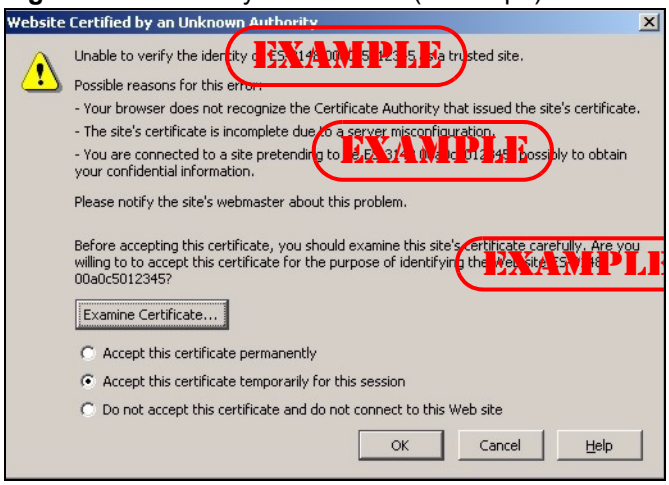

Website Certified by an Unknown Authority
Unable to verify the identity of
Possible reasons for this error:
- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to
your confidential information.
Please notify the site's webmaster about this problem.
Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying
00a0c5012345?
Examine Certificate...
Accept this certificate permanently
Accept this certificate temporarily for this session
Do not accept this certificate and do not connect to this Web site
OK
Cancel
Help
EXAMPLE
EXAMPLE
EXAMPLE

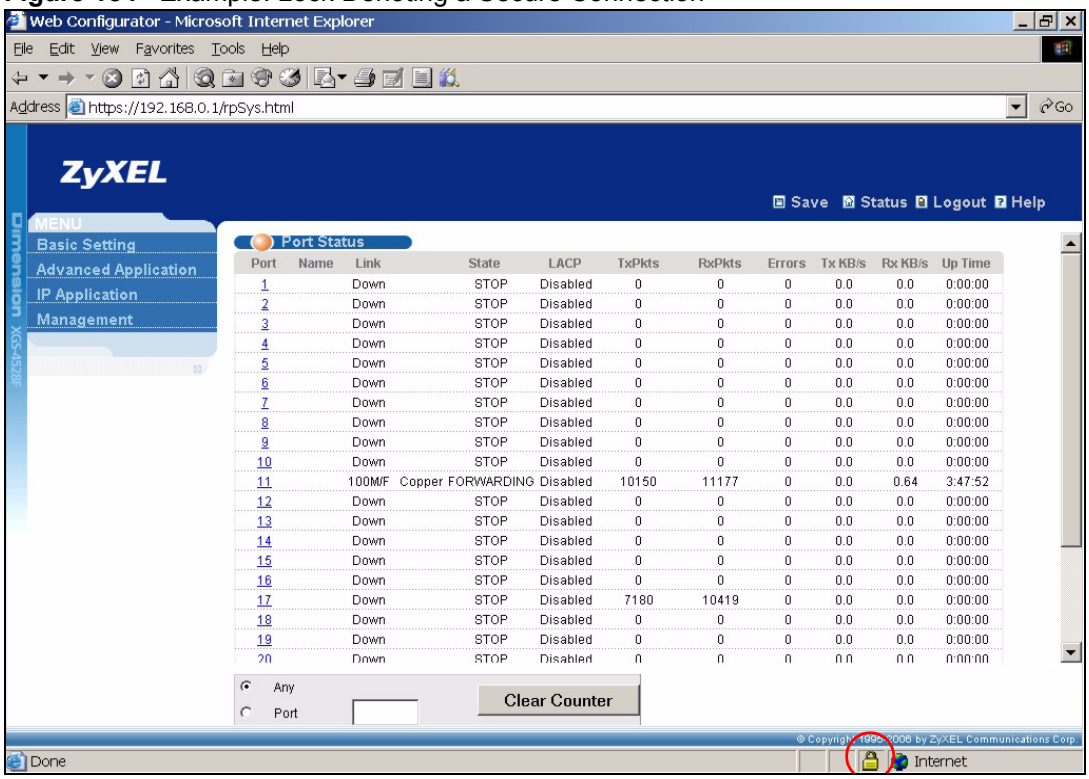
Figure 183 Security Certificate 2 (Netscape)

Security Error: Domain Name Mismatch
You have attempted to establish a connection with
"192.168.1.1". However, the security certificate presented
belongs to
communication with this web site.
If you suspect the certificate shown does not belong to
"192.168.1.1", please cancel the connection and notify the site
administrator.
View Certificate
OK
Cancel
Help
EXAMPLE

35.8.3 The Main Screen

After you accept the certificate and enter the login username and password, the Switch main screen appears. The lock displayed in the bottom right of the browser status bar denotes a secure connection.

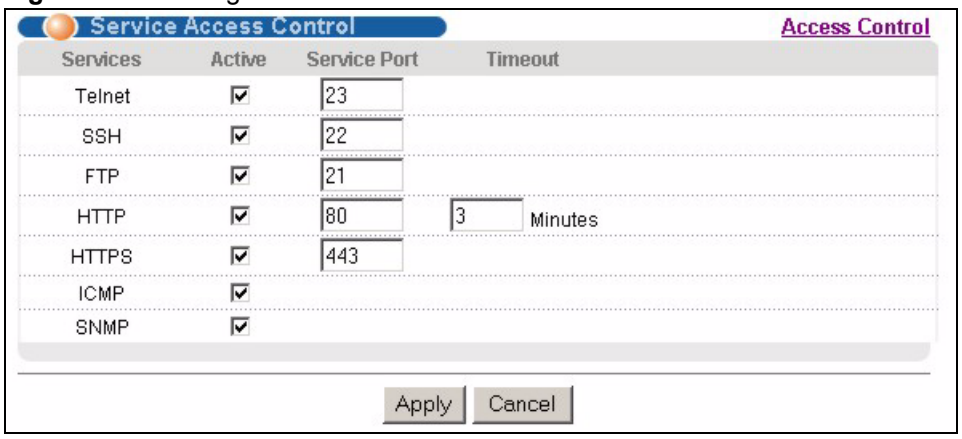
Figure 184 Example: Lock Denoting a Secure Connection



35.9 Service Port Access Control

Service Access Control allows you to decide what services you may use to access the Switch. You may also change the default service port and configure “trusted computer(s)” for each service in the **Remote Management** screen (discussed later). Click **Access Control** to go back to the main **Access Control** screen.

Figure 185 Management > Access Control > Service Access Control



The following table describes the fields in this screen.

Table 123 Management > Access Control > Service Access Control

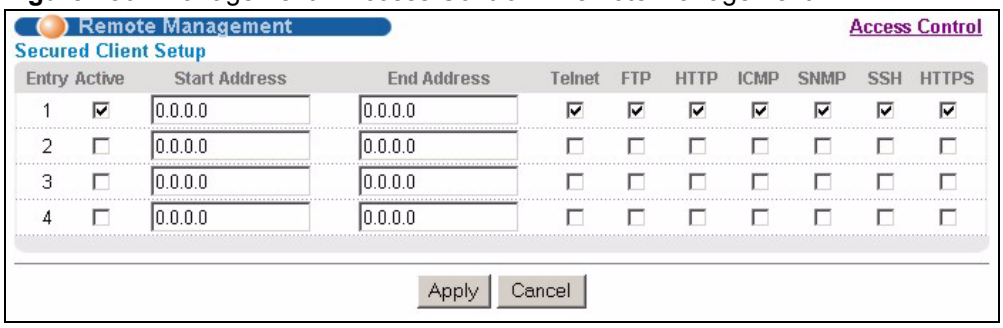
LABEL	DESCRIPTION
Services	Services you may use to access the Switch are listed here.
Active	Select this option for the corresponding services that you want to allow to access the Switch.
Service Port	For Telnet, SSH, FTP, HTTP or HTTPS services, you may change the default service port by typing the new port number in the **Server Port** field. If you change the default port number then you will have to let people (who wish to use the service) know the new port number for that service.
Timeout	Type how many minutes a management session (via the web configurator) can be left idle before the session times out. After it times out you have to log in with your password again. Very long idle timeouts may have security risks.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

35.10 Remote Management

From the **Access Control** screen, display the **Remote Management** screen as shown next.

You can specify a group of one or more "trusted computers" from which an administrator may use a service to manage the Switch. Click **Access Control** to return to the **Access Control** screen.

Figure 186 Management > Access Control > Remote Management



The following table describes the labels in this screen.

Table 124 Management > Access Control > Remote Management

LABEL	DESCRIPTION
Entry	This is the client set index number. A "client set" is a group of one or more "trusted computers" from which an administrator may use a service to manage the Switch.
Active	Select this check box to activate this secured client set. Clear the check box if you wish to temporarily disable the set without deleting it.
Start Address End Address	Configure the IP address range of trusted computers from which you can manage this Switch. The Switch checks if the client IP address of a computer requesting a service or protocol matches the range set here. The Switch immediately disconnects the session if it does not match.

Table 124 Management > Access Control > Remote Management (continued)

LABEL	DESCRIPTION
Telnet/FTP/ HTTP/ICMP/ SNMP/SSH/ HTTPS	Select services that may be used for managing the Switch from the specified trusted computers.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

36

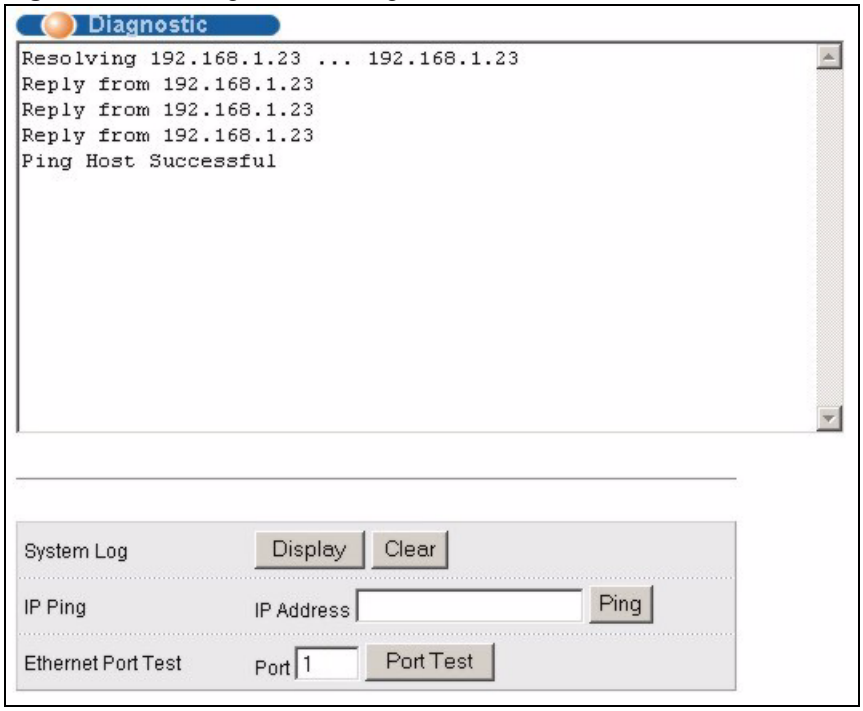
Diagnostic

This chapter explains the **Diagnostic** screen.

36.1 Diagnostic

Click **Management** > **Diagnostic** in the navigation panel to open this screen. Use this screen to check system logs, ping IP addresses or perform port tests.

Figure 187 Management > Diagnostic



The following table describes the labels in this screen.

Table 125 Management > Diagnostic

LABEL	DESCRIPTION
System Log	Click **Display** to display a log of events in the multi-line text box. Click **Clear** to empty the text box and reset the syslog entry.
IP Ping	Type the IP address of a device that you want to ping in order to test a connection. Click **Ping** to have the Switch ping the IP address (in the field to the left).
Ethernet Port Test	Enter a port number and click **Port Test** to perform an internal loopback test.

37 Syslog

This chapter explains the syslog screens.

37.1 Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

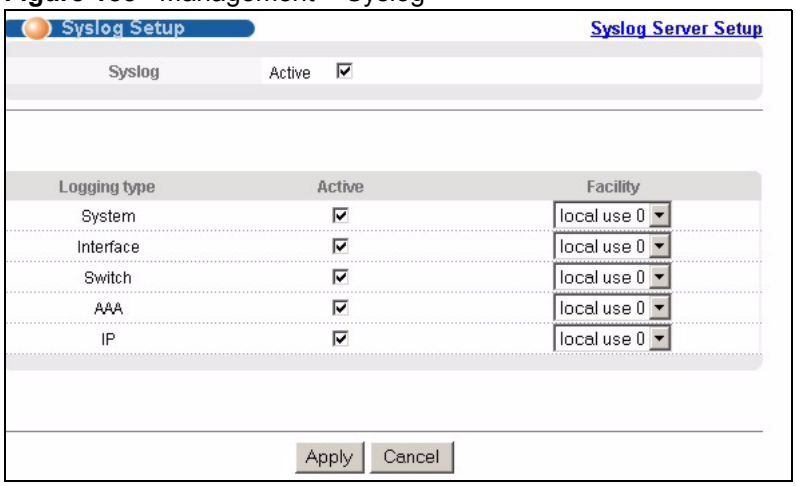
Table 126 Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

37.2 Syslog Setup

Click **Management** > **Syslog** in the navigation panel to display this screen. The syslog feature sends logs to an external syslog server. Use this screen to configure the device's system logging settings.

Figure 188 Management > Syslog



The following table describes the labels in this screen.

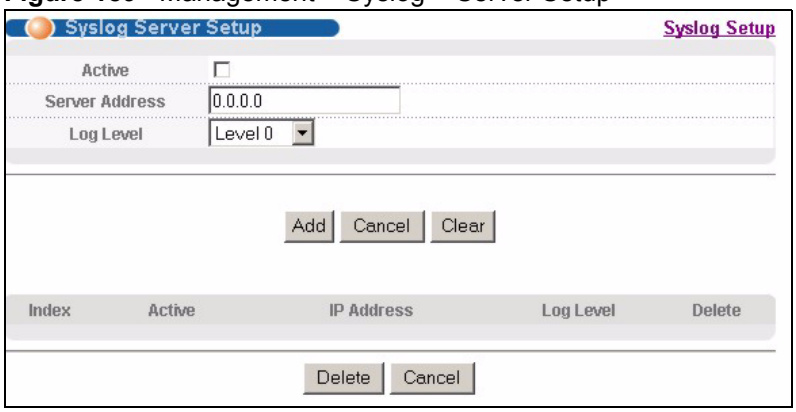
Table 127 Management > Syslog

LABEL	DESCRIPTION
Syslog	Select **Active** to turn on syslog (system logging) and then configure the syslog setting
Logging Type	This column displays the names of the categories of logs that the device can generate.
Active	Select this option to set the device to generate logs for the corresponding category.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

37.3 Syslog Server Setup

Click **Management** > **Syslog** > **Syslog Server Setup** to open the following screen. Use this screen to configure a list of external syslog servers.

Figure 189 Management > Syslog > Server Setup



The following table describes the labels in this screen.

Table 128 Management > Syslog > Server Setup

LABEL	DESCRIPTION
Active	Select this check box to have the device send logs to this syslog server. Clear the check box if you want to create a syslog server entry but not have the device send logs to it (you can edit the entry later).
Server Address	Enter the IP address of the syslog server.
Log Level	Select the severity level(s) of the logs that you want the device to send to this syslog server. The lower the number, the more critical the logs are.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to return the fields to the factory defaults.
Index	This is the index number of a syslog server entry. Click this number to edit the entry.
Active	This field displays **Yes** if the device is to send logs to the syslog server. **No** displays if the device is not to send logs to the syslog server.
IP Address	This field displays the IP address of the syslog server.
Log Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Delete	Select an entry's **Delete** check box and click **Delete** to remove the entry.
Cancel	Click **Cancel** to begin configuring this screen afresh.

38

Cluster Management

This chapter introduces cluster management.

38.1 Clustering Management Status Overview

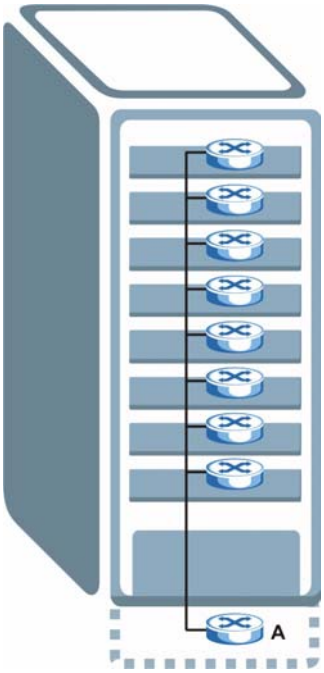
Cluster Management allows you to manage switches through one Switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 129 ZyXEL Clustering Management Specifications

Maximum number of cluster members	24
Cluster Member Models	Cluster member models must be compatible with ZyXEL cluster management implementation.
Cluster Manager	The cluster manager is the Switch through which you manage the cluster member switches.
Cluster Members	Cluster members are the switches being managed by the cluster manager switch.

In the following example, switch **A** in the basement is the cluster manager and the other switches on the upper floors of the building are cluster members.

Figure 190 Clustering Application Example

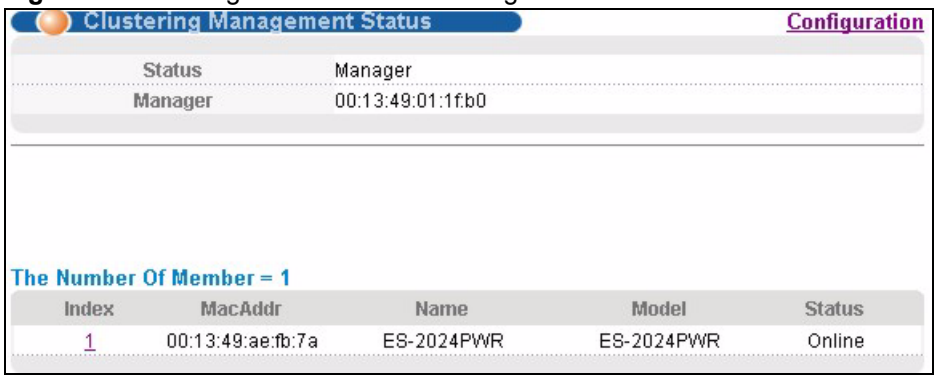


38.2 Cluster Management Status

Click **Management** > **Cluster Management** in the navigation panel to display the following screen.

A cluster can only have one manager.

Figure 191 Management > Cluster Management



The following table describes the labels in this screen.

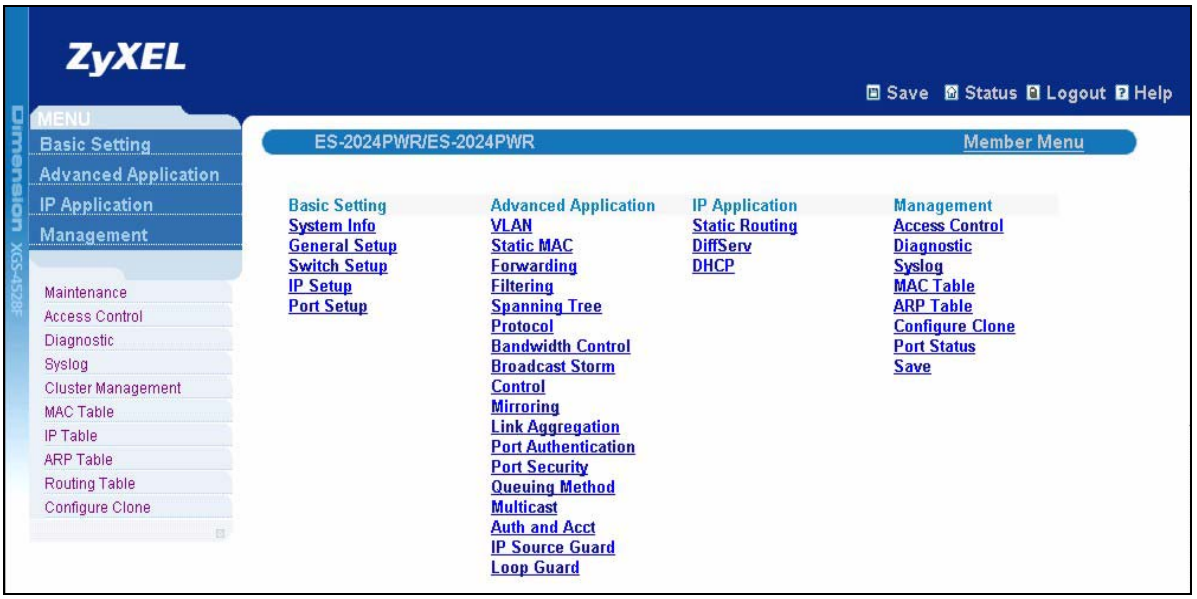
Table 130 Management > Cluster Management

LABEL	DESCRIPTION
Status	This field displays the role of this Switch within the cluster. **Manager** **Member** (you see this if you access this screen in the cluster member switch directly and not via the cluster manager) **None** (neither a manager nor a member of a cluster)
Manager	This field displays the cluster manager switch's hardware MAC address.
The Number of Member	This field displays the number of switches that make up this cluster. The following fields describe the cluster member switches.
Index	You can manage cluster member switches via the cluster manager switch. Each number in the **Index** column is a hyperlink leading to the cluster member switch's web configurator (see Figure 192 on page 311).
MacAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's **System Name**.
Model	This field displays the model name.
Status	This field displays: **Online** (the cluster member switch is accessible) **Error** (for example, the cluster member switch password was changed or the switch was set as the manager and so left the member list, etc.) **Offline** (the switch is disconnected - **Offline** shows approximately 1.5 minutes after the link between cluster member and manager goes down)

38.2.1 Cluster Member Switch Management

Go to the **Clustering Management Status** screen of the cluster manager switch and then select an **Index** hyperlink from the list of members to go to that cluster member switch's web configurator home page. This cluster member web configurator home page and the home page that you'd see if you accessed it directly are different.

Figure 192 Cluster Management: Cluster Member Web Configurator Screen



38.2.1.1 Uploading Firmware to a Cluster Member Switch

You can use FTP to upload firmware to a cluster member switch through the cluster manager switch as shown in the following example.

Figure 193 Example: Uploading Firmware to a Cluster Member Switch

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 Switch FTP version 1.0 ready at Thu Jan  1 00:58:46 1970
User (192.168.0.1:(none)): admin
331 Enter PASS command
Password:
230 Logged in
ftp> ls
200 Port command okay
150 Opening data connection for LIST
--w--w--w-   1 owner    group         3042210 Jul 01 12:00 ras
-rw-rw-rw-   1 owner    group          393216 Jul 01 12:00 config
--w--w--w-   1 owner    group               0 Jul 01 12:00 fw-00-a0-c5-01-23-46
-rw-rw-rw-   1 owner    group               0 Jul 01 12:00 config-00-a0-c5-01-23-46
226 File sent OK
ftp: 297 bytes received in 0.00Seconds 297000.00Kbytes/sec.
ftp> bin
200 Type I OK
ftp> put 370lt0.bin fw-00-a0-c5-01-23-46
200 Port command okay
150 Opening data connection for STOR fw-00-a0-c5-01-23-46
226 File received OK
ftp: 262144 bytes sent in 0.63Seconds 415.44Kbytes/sec.
ftp>
```

The following table explains some of the FTP parameters.

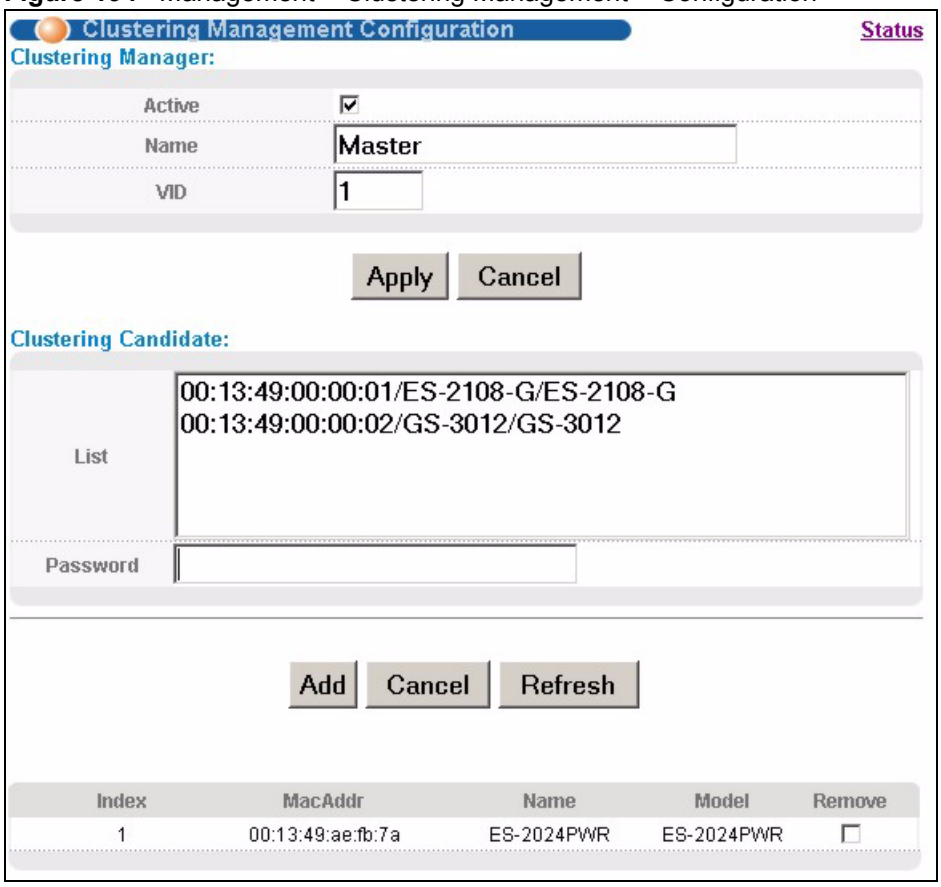
Table 131 FTP Upload to Cluster Member Example

FTP PARAMETER	DESCRIPTION
`User`	Enter “admin”.
`Password`	The web configurator password default is 1234.
`ls`	Enter this command to list the name of cluster member switch’s firmware and configuration file.
`370lt0.bin`	This is the name of the firmware file you want to upload to the cluster member switch.
`fw-00-a0-c5-01-23-46`	This is the cluster member switch’s firmware name as seen in the cluster manager switch.
`config-00-a0-c5-01-23-46`	This is the cluster member switch’s configuration file name as seen in the cluster manager switch.

38.3 Clustering Management Configuration

Use this screen to configure clustering management. Click **Configuration** from the **Cluster Management** screen to display the next screen.

Figure 194 Management > Clustering Management > Configuration



The following table describes the labels in this screen.

Table 132 Management > Clustering Management > Configuration

LABEL	DESCRIPTION
Clustering Manager	
Active	Select **Active** to have this Switch become the cluster manager switch. A cluster can only have one manager. Other (directly connected) switches that are set to be cluster managers will not be visible in the **Clustering Candidates** list. If a switch that was previously a cluster member is later set to become a cluster manager, then its **Status** is displayed as **Error** in the **Cluster Management Status** screen and a warning icon (⚠) appears in the member summary list below.
Name	Type a name to identify the **Clustering Manager.** You may use up to 32 printable characters (spaces are allowed).
VID	This is the VLAN ID and is only applicable if the Switch is set to **802.1Q** VLAN. All switches must be directly connected and in the same VLAN group to belong to the same cluster. Switches that are not in the same VLAN group are not visible in the **Clustering Candidates** list. This field is ignored if the **Clustering Manager** is using **Port-based** VLAN.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Table 132 Management > Clustering Management > Configuration (continued)

LABEL	DESCRIPTION
Clustering Candidate	The following fields relate to the switches that are potential cluster members.
List	A list of suitable candidates found by auto-discovery is shown here. The switches must be directly connected. Directly connected switches that are set to be cluster managers will not be visible in the **Clustering Candidate** list. Switches that are not in the same management VLAN group will not be visible in the **Clustering Candidate** list.
Password	Each cluster member's password is its web configurator password. Select a member in the **Clustering Candidate** list and then enter its web configurator password. If that switch administrator changes the web configurator password afterwards, then it cannot be managed from the **Cluster Manager**. Its **Status** is displayed as **Error** in the **Cluster Management Status** screen and a warning icon (⚠) appears in the member summary list below. If multiple devices have the same password then hold [SHIFT] and click those switches to select them. Then enter their common web configurator password.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Refresh	Click **Refresh** to perform auto-discovery again to list potential cluster members.
The next summary table shows the information for the clustering members configured.	
Index	This is the index number of a cluster member switch.
MacAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's **System Name**.
Model	This is the cluster member switch's model name.
Remove	Select this checkbox and then click the **Remove** button to remove a cluster member switch from the cluster.
Cancel	Click **Cancel** to begin configuring this screen afresh.

39

MAC Table

This chapter introduces the **MAC Table** screen.

39.1 MAC Table Overview

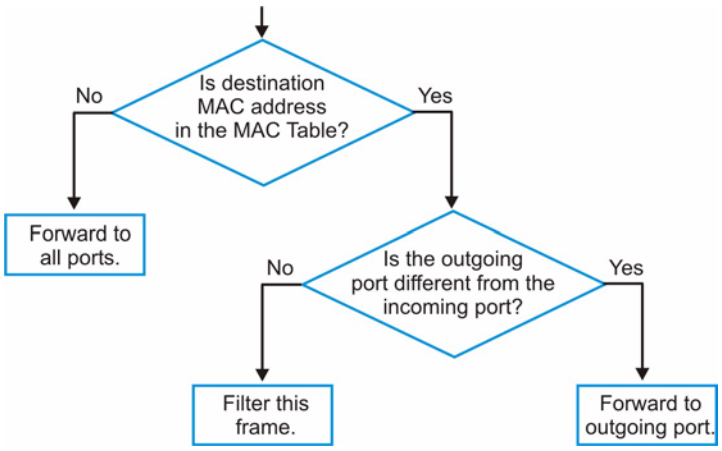
The **MAC Table** screen (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the Switch's ports. When a device (which may belong to a VLAN group) sends a packet which is forwarded to a port on the Switch, the MAC address of the device is shown on the Switch's **MAC Table**. It also shows whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the **Static MAC Forwarding** screen).

The Switch uses the **MAC Table** to determine how to forward frames. See the following figure.

1. The Switch examines a received frame and learns the port from which this source MAC address came.
2. The Switch checks to see if the frame's destination MAC address matches a source MAC address already learned in the **MAC Table**.

- If the Switch has already learned the port for this MAC address, then it forwards the frame to that port.
- If the Switch has not already learned the port for this MAC address, then the frame is flooded to all ports. Too much port flooding leads to network congestion.
- If the Switch has already learned the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.

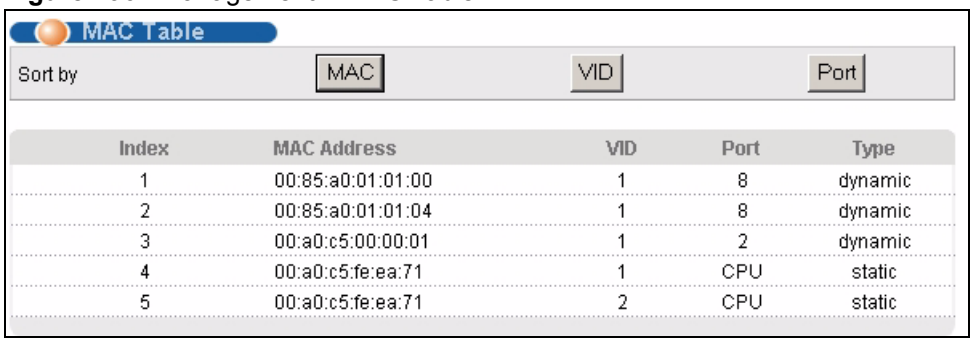
Figure 195 MAC Table Flowchart



39.2 Viewing the MAC Table

Click **Management** > **MAC Table** in the navigation panel to display the following screen.

Figure 196 Management > MAC Table



The following table describes the labels in this screen.

Table 133 Management > MAC Table

LABEL	DESCRIPTION
Sort by	Click one of the following buttons to display and arrange the data according to that button type. The information is then displayed in the summary table below.
MAC	Click this button to display and arrange the data according to MAC address.
VID	Click this button to display and arrange the data according to VLAN group.
Port	Click this button to display and arrange the data according to port number.
Index	This is the incoming frame index number.
MAC Address	This is the MAC address of the device from which this incoming frame came.
VID	This is the VLAN group to which this frame belongs.
Port	This is the port from which the above MAC address was learned.
Type	This shows whether the MAC address is **dynamic** (learned by the Switch) or **static** (manually entered in the **Static MAC Forwarding** screen).

40

IP Table

This chapter introduces the IP table.

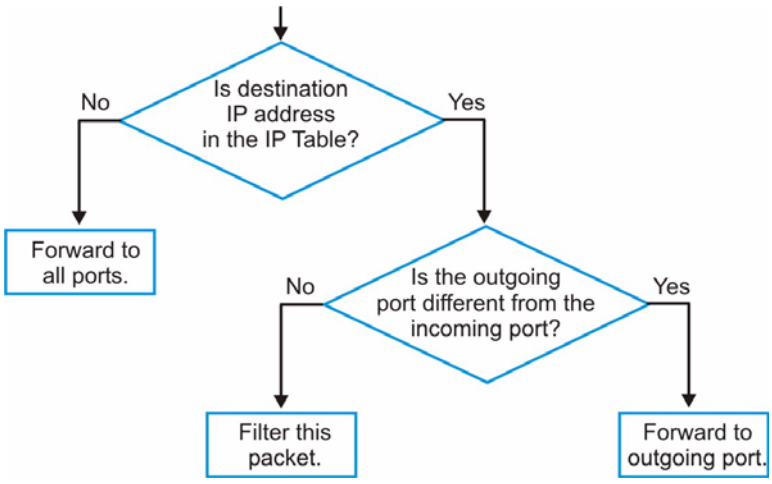
40.1 IP Table Overview

The **IP Table** screen shows how packets are forwarded or filtered across the Switch's ports. When a device (which may belong to a VLAN group) sends a packet which is forwarded to a port on the Switch, the IP address of the device is shown on the Switch's **IP Table**. The **IP Table** also shows whether the IP address is dynamic (learned by the Switch) or static (belonging to the Switch).

The Switch uses the **IP Table** to determine how to forward packets. See the following figure.

1. The Switch examines a received packet and learns the port from which this source IP address came.
2. The Switch checks to see if the packet's destination IP address matches a source IP address already learned in the **IP Table**.
   - If the Switch has already learned the port for this IP address, then it forwards the packet to that port.
   - If the Switch has not already learned the port for this IP address, then the packet is flooded to all ports. Too much port flooding leads to network congestion.
   - If the Switch has already learned the port for this IP address, but the destination port is the same as the port it came in on, then it filters the packet.

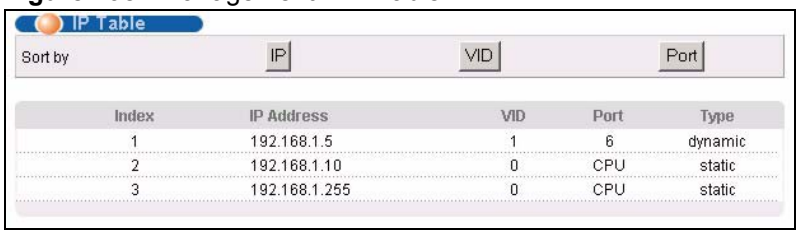
Figure 197 IP Table Flowchart



40.2 Viewing the IP Table

Click **Management** > **IP Table** in the navigation panel to display the following screen.

Figure 198 Management > IP Table



The following table describes the labels in this screen.

Table 134 Management > IP Table

LABEL	DESCRIPTION
Sort by	Click one of the following buttons to display and arrange the data according to that button type. The information is then displayed in the summary table below.
IP	Click this button to display and arrange the data according to IP address.
VID	Click this button to display and arrange the data according to VLAN group.
Port	Click this button to display and arrange the data according to port number.
Index	This field displays the index number.
IP Address	This is the IP address of the device from which the incoming packets came.
VID	This is the VLAN group to which the packet belongs.
Port	This is the port from which the above IP address was learned. This field displays **CPU** to indicate the IP address belongs to the Switch.
Type	This shows whether the IP address is **dynamic** (learned by the Switch) or **static** (belonging to the Switch).

41

ARP Table

This chapter introduces ARP Table.

41.1 ARP Table Overview

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

41.1.1 How ARP Works

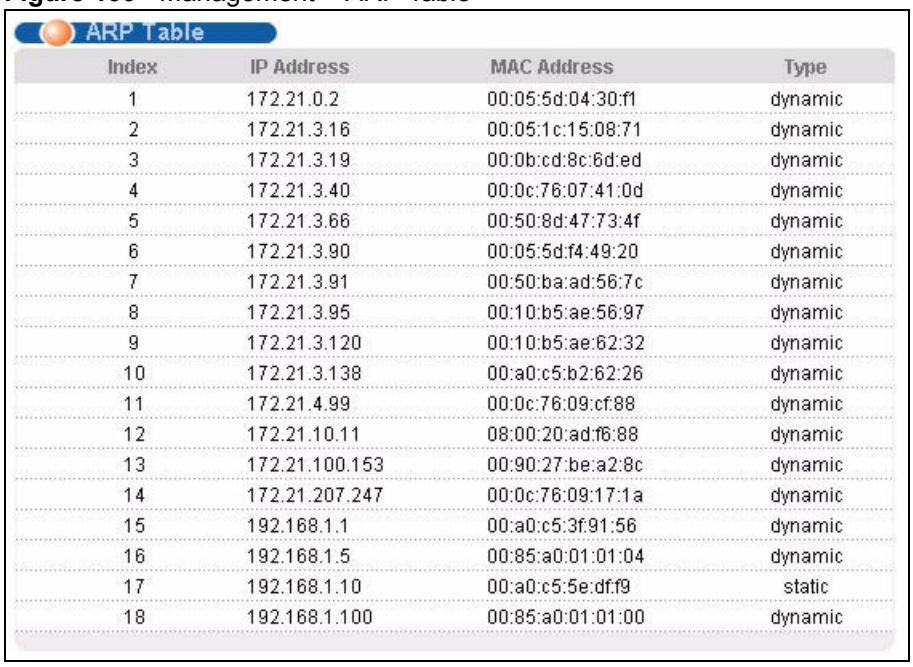
When an incoming packet destined for a host device on a local area network arrives at the Switch, the Switch's ARP program looks in the ARP Table and if it finds the address, it sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The Switch fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the Switch puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

41.2 Viewing the ARP Table

Click **Management** > **ARP Table** in the navigation panel to open the following screen. Use the ARP table to view IP-to-MAC address mapping(s).

Figure 199 Management > ARP Table



The following table describes the labels in this screen.

Table 135 Management > ARP Table

LABEL	DESCRIPTION
Index	This is the ARP Table entry number.
IP Address	This is the learned IP address of a device connected to a Switch port with the corresponding MAC address below.
MAC Address	This is the MAC address of the device with the corresponding IP address above.
Type	This shows whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the **Static MAC Forwarding** screen).

42

Routing Table

This chapter introduces the routing table.

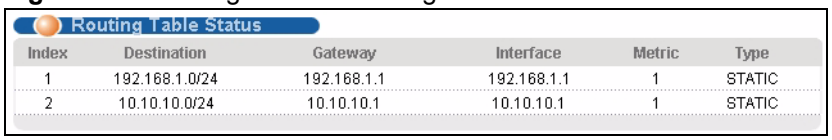
42.1 Overview

The routing table contains the route information to the network(s) that the Switch can reach. The Switch automatically updates the routing table with the RIP information received from other Ethernet devices.

42.2 Viewing the Routing Table Status

Use this screen to view routing table information. Click **Management** > **Routing Table** in the navigation panel to display the screen as shown.

Figure 200 Management > Routing Table



The following table describes the labels in this screen.

Table 136 Management > Routing Table

LABEL	DESCRIPTION
Index	This field displays the index number.
Destination	This field displays the destination IP routing domain.
Gateway	This field displays the IP address of the gateway device.
Interface	This field displays the IP address of the Interface.
Metric	This field displays the cost of the route.
Type	This field displays the method used to learn the route; **OSPF** - added as an OSPF interface, **RIP** - learned from incoming RIP packets or **STATIC** - added as a static entry.

43

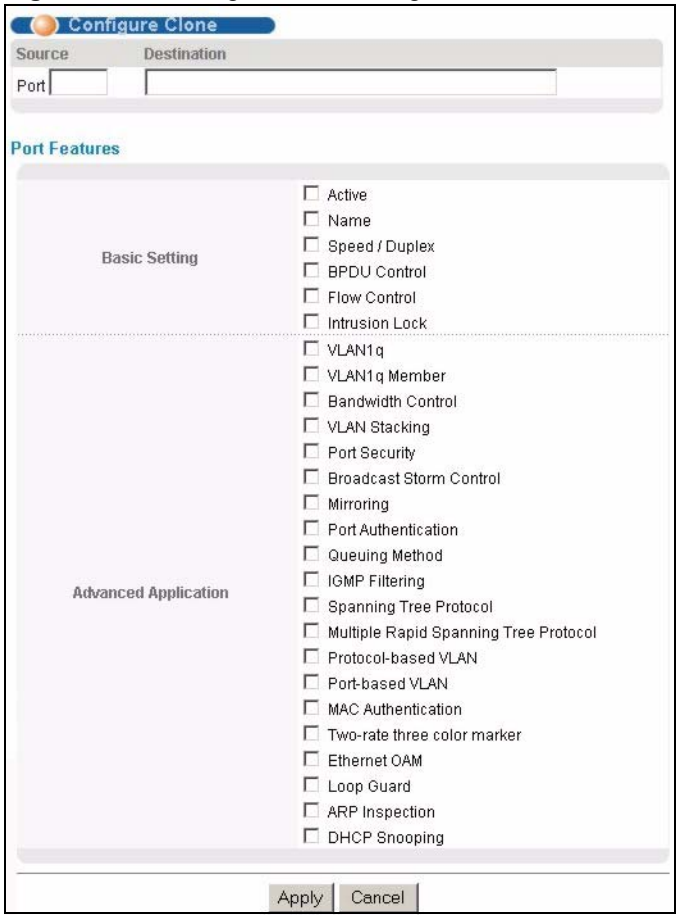
Configure Clone

This chapter shows you how you can copy the settings of one port onto other ports.

43.1 Configure Clone

Cloning allows you to copy the basic and advanced settings from a source port to a destination port or ports. Click **Management** > **Configure Clone** to open the following screen.

Figure 201 Management > Configure Clone



The following table describes the labels in this screen.

Table 137 Management > Configure Clone

LABEL	DESCRIPTION
Source/ Destination Port	Enter the source port under the **Source** label. This port's attributes are copied. Enter the destination port or ports under the **Destination** label. These are the ports which are going to have the same attributes as the source port. You can enter individual ports separated by a comma or a range of ports by using a dash. Example: • **2, 4, 6** indicates that ports 2, 4 and 6 are the destination ports. • **2-6** indicates that ports 2 through 6 are the destination ports.
Basic Setting	Select which port settings (configured in the **Basic Setting** menus) should be copied to the destination port(s).
Advanced Application	Select which port settings (configured in the **Advanced Application** menus) should be copied to the destination ports.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

PART VI
Troubleshooting & Product Specifications

Troubleshooting (327)
Product Specifications (335)

44

Troubleshooting

This chapter covers potential problems and possible remedies.

44.1 Problems Starting Up the Switch

Table 138 Troubleshooting the Start-Up of Your Switch

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when you turn on the Switch.	Check the power connection and make sure the power source is turned on.
	If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

44.2 Problems Accessing the Switch

Table 139 Troubleshooting Accessing the Switch

PROBLEM	CORRECTIVE ACTION
I cannot access the Switch using Telnet.	Make sure the ports are properly connected. You may have exceeded the maximum number of concurrent Telnet sessions. Close other Telnet session(s) or try connecting again later. Check that you have enabled Telnet service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on access control for details.
I cannot access the web configurator.	The administrator username is "admin". The default administrator password is "1234". The username and password are case-sensitive. Make sure that you enter the correct password and username using the proper casing. If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This restores all of the factory defaults including the password. If you have configured more than one IP interface, make sure another administrator is NOT logged into the web configurator on a different IP interface using the same account. Check that you have enabled web service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on access control for details. Your computer's and the Switch's IP addresses must be on the same subnet. See the following section to check that pop-up windows, JavaScripts and Java permissions are allowed.

44.2.1 Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

44.2.1.1 Internet Explorer Pop-up Blockers

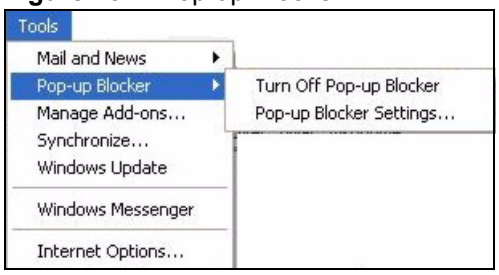
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

44.2.1.1.1 Disable pop-up Blockers

1. In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

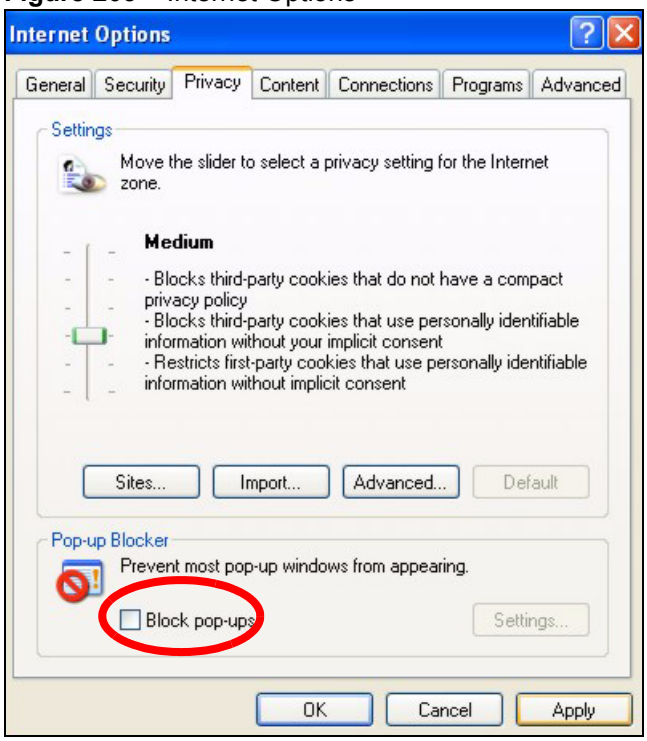
Figure 202 Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1. In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.
2. Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 203 Internet Options



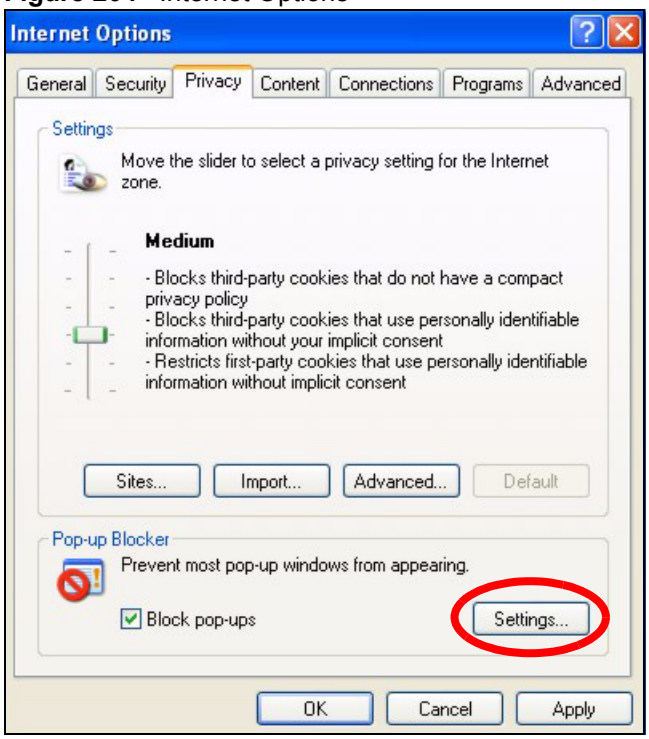
3 Click **Apply** to save this setting.

44.2.1.1.2 Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.
2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

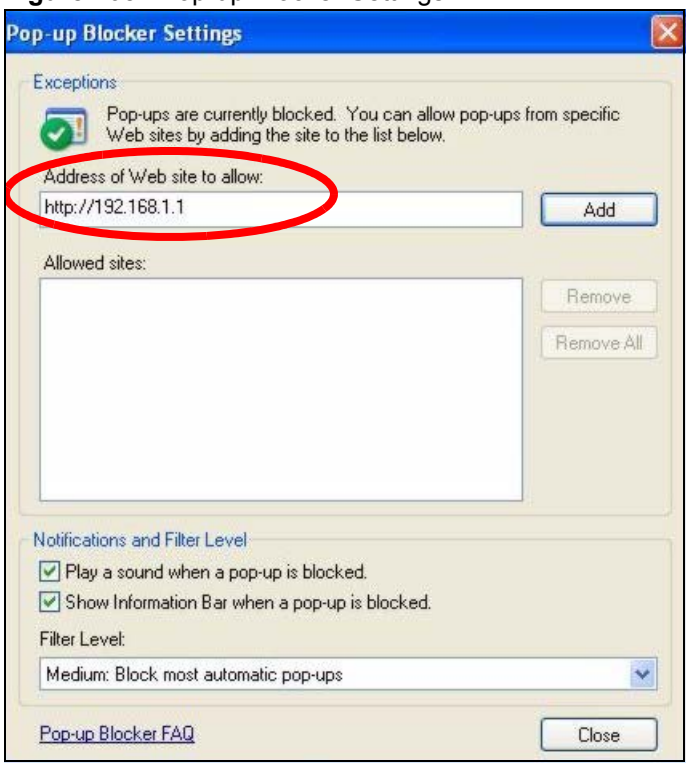
Figure 204 Internet Options



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.1.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 205 Pop-up Blocker Settings


Pop-up Blocker Settings
Exceptions
Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.
Address of Web site to allow:
http://192.168.1.1
Add
Allowed sites:
Remove
Remove All
Notifications and Filter Level
Play a sound when a pop-up is blocked.
Show Information Bar when a pop-up is blocked.
Filter Level:
Medium: Block most automatic pop-ups
Pop-up Blocker FAQ
Close

5 Click **Close** to return to the **Privacy** screen.

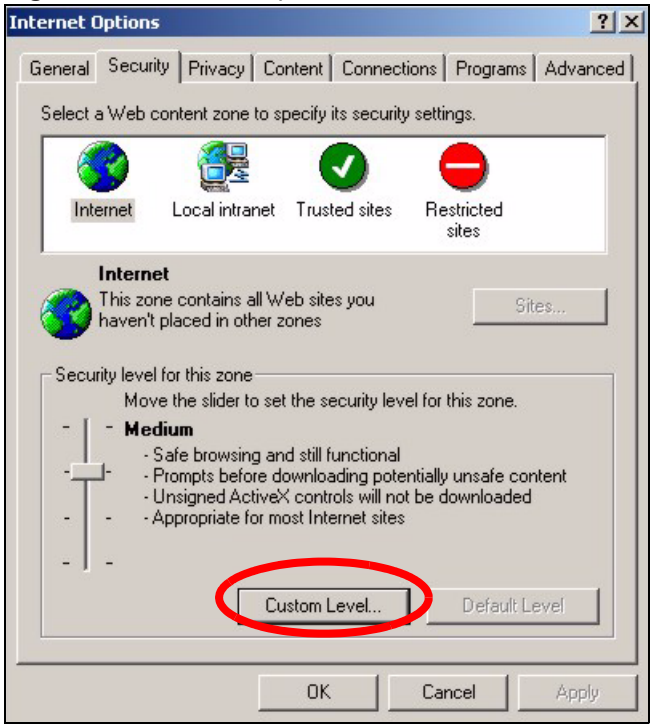
6 Click **Apply** to save this setting.

44.2.1.2 JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 206 Internet Options



2 Click the **Custom Level...** button.

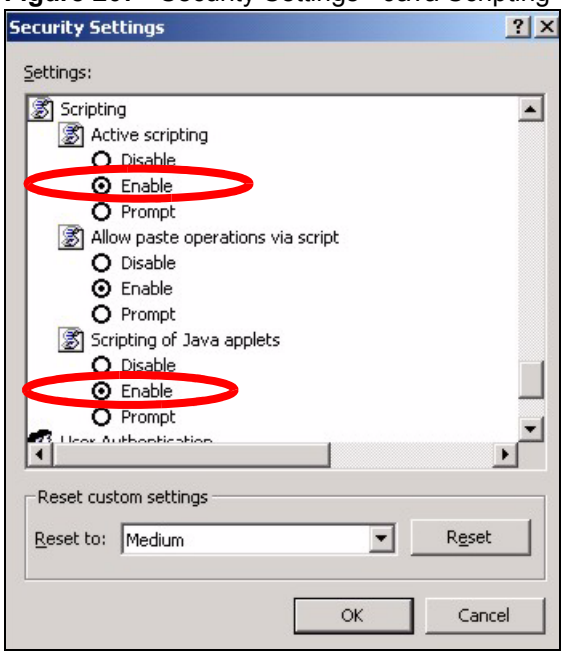
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

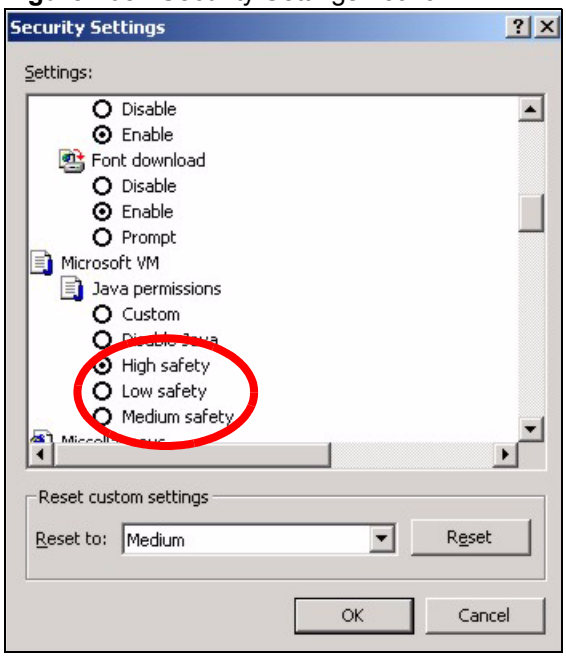
Figure 207 Security Settings - Java Scripting



44.2.1.3 Java Permissions

1. From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.
2. Click the **Custom Level...** button.
3. Scroll down to **Microsoft VM**.
4. Under **Java permissions** make sure that a safety level is selected.
5. Click **OK** to close the window.

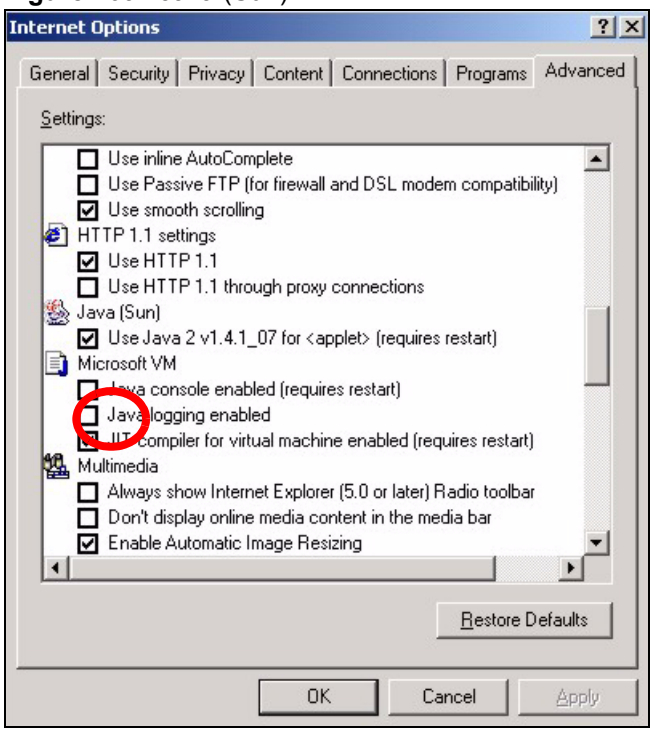
Figure 208 Security Settings - Java



44.2.1.3.1 JAVA (Sun)

1. From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.
2. Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
3. Click **OK** to close the window.

Figure 209 Java (Sun)



44.3 Problems with the Password

Table 140 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
Cannot access the Switch.	The password field is case sensitive. Make sure that you enter the correct password using the proper casing.
	The administrator username is “admin”. The default administrator password is “1234”. The username and password are case-sensitive. Make sure that you enter the correct password and username using the proper casing. If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This restores all of the factory defaults including the password.

45

Product Specifications

The following tables summarize the Switch's hardware and firmware features.

Table 141 Hardware Specifications

SPECIFICATION	DESCRIPTION
Dimensions	Standard 19" rack mountable 438 mm (W) x 310 mm (D) x 44.45 mm (H)
Weight	4.9 Kg
Power Specification	AC: 100 - 240 VAC 50/60 Hz 0.8 A max, 85 W internal universal power supply DC: -36 VDC ~ -72 VDC 2.3 A max, 80 W consumption. There is no tolerance for the DC input voltage. One Backup Power Supply (BPS) connector
Interfaces	24 Gigabit Ethernet (GbE) Dual Personality interfaces. Each interface has: -a 1000Base-T port, compatible with Cat5/5e/6 copper cable. -a mini-GBIC slot, compatible with Small Form-Factor Pluggable (SFP) Multi Source Agreement (MSA) transceivers, to be used with 1000Base-X fiber cables. For each Dual Personality interface one port or slot is active at a time. Two stacking ports One optional uplink module set. One local management Ethernet 10/100Base-T port One RS-232 console port
Ethernet Ports	Auto-negotiating: 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode. 1000 Mbps and 10 Gbps in full duplex. Auto-crossover: Use either crossover or straight-through Ethernet cables. Auto-MDIX Compliant with IEEE 802.3ad/u/x Back pressure flow control for half duplex Flow control for full duplex (IEEE 802.3x)
LEDs	Main switch: BPS, PWR, SYS, ALM, Per Stacking port: S1, S2 Per mini-GBIC port: green LED Per 1000Base-T port: Green: 10/1000 Mbps Amber: 100 Mbps mini-GBIC/1000Base-T LEDs: steady: link state blinking: transmitting/receiving
Operating Environment	Temperature: 0º C ~ 45º C (32º F ~ 113º F) Humidity: 10 ~ 90% (non-condensing)
Storage Environment	Temperature: -25º C ~ 70º C (-13º F ~ 158º F) Humidity: 10 ~ 90% (non-condensing)

Table 141 Hardware Specifications

Ground Wire Gauge	18 AWG or larger
Power Wire Gauge	18 AWG or larger
Fuse Specification	250 VAC, T4A. For DC version switchboard.
Approvals	Safety UL 60950-1, CSA 60950-1, EN 60950-1, IEC 60950-1 EMC FCC Part 15 (Class A), CE EMC (Class A)

Table 142 Firmware Specifications

FEATURE	DESCRIPTION
Default IP Address	In band: 192.168.1.1 Out of band (Management port): 192.168.0.1
Default Subnet Mask	255.255.255.0 (24 bits)
Administrator User Name	admin
Default Password	1234
Number of Login Accounts Configurable on the Switch	4 management accounts configured on the Switch. Authentication via RADIUS and TACACS+ also available.
IP Routing Domain	An IP interface (also known as an IP routing domain) is not bound to a physical port. Configure an IP routing domain to allow the Switch to route traffic between different networks.
VLAN	A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.
VLAN Stacking	Use VLAN stacking to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter the network. By tagging the tagged frames (“double-tagged” frames), the service provider can manage up to 4,094 VLAN groups with each group containing up to 4,094 customer VLANs. This allows a service provider to provide different service, based on specific VLANs, for many different customers.
MAC Address Filter	Filter traffic based on the source and/or destination MAC address and VLAN group (ID).
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the Switch assign IP addresses, an IP default gateway and DNS servers to computers on your network.
IGMP Snooping	The Switch supports IGMP snooping enabling group multicast traffic to be only forwarded to ports that are members of that group; thus allowing you to significantly reduce multicast traffic passing through your Switch.
Differentiated Services (DiffServ)	With DiffServ, the Switch marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow.
Classifier and Policy	You can create a policy to define actions to be performed on a traffic flow grouped by a classifier according to specific criteria such as the IP address, port number or protocol type, etc.

Table 142 Firmware Specifications

FEATURE	DESCRIPTION
Queuing	Queuing is used to help solve performance degradation when there is network congestion. Three scheduling services are supported: Strict Priority Queuing (SPQ), Weighted Round Robin (WRR) and Weighted Fair Queuing (WFQ). This allows the Switch to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.
Port Mirroring	Port mirroring allows you to copy traffic going from one or all ports to another or all ports in order that you can examine the traffic from the mirror port (the port you copy the traffic to) without interference.
Static Route	Static routes tell the Switch how to forward IP traffic when you configure the TCP/IP parameters manually.
Multicast VLAN Registration (MVR)	Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) using multicast traffic across a network. MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network. This improves bandwidth utilization by reducing multicast traffic in the subscriber VLANs and simplifies multicast group management.
IP Multicast	With IP multicast, the Switch delivers IP packets to a group of hosts on the network - not everybody. In addition, the Switch can send packets to Ethernet devices that are not VLAN-aware by untagging (removing the VLAN tags) IP multicast packets.
RIP	RIP (Routing Information Protocol) allows a routing device to exchange routing information with other routers.
OSPF	OSPF (Open Shortest Path First) is a link-state protocol designed to distribute routing information within an autonomous system (AS). An autonomous system is a collection of networks using a common routing protocol to exchange routing information. OSPF is best suited for large networks.
DVMRP	DVMRP (Distance Vector Multicast Routing Protocol) is a protocol used for routing multicast data within an autonomous system (AS). DVMRP provides multicast forwarding capability to a layer 3 switch that runs both the IPv4 protocol (with IP Multicast support) and the IGMP protocol.
VRRP	Virtual Router Redundancy Protocol (VRRP), defined in RFC 2338, allows you to create redundant backup gateways to ensure that the default gateway of a host is always available.
STP (Spanning Tree Protocol) / RSTP (Rapid STP)	(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a Switch to interact with other (R)STP -compliant switches in your network to ensure that only one path exists between any two stations on the network.
Loop Guard	Use the loop guard feature to protect against network loops on the edge of your network.
IP Source Guard	Use IP source guard to filter unauthorized DHCP and ARP packets in your network.
Link Aggregation	Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.
Port Authentication and Security	For security, the Switch allows authentication using IEEE 802.1x with an external RADIUS server and port security that allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the Switch.

Table 142 Firmware Specifications

FEATURE	DESCRIPTION
Authentication and Accounting	The Switch supports authentication and accounting services via RADIUS and TACACS+ AAA servers.
Device Management	Use the web configurator or commands to easily configure the rich range of features on the Switch.
Port Cloning	Use the port cloning feature to copy the settings you configure on one port to another port or ports.
Syslog	The Switch can generate syslog messages and send it to a syslog server.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator, CLI or an FTP/TFTP tool to put it on the Switch. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the Switch's configuration and put it back on the Switch later if you decide you want to revert back to an earlier configuration.
Cluster Management	Cluster management (also known as iStacking) allows you to manage switches through one switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 143 Switching Specifications

Layer 2 Features	Bridging	8K MAC addresses Static MAC address filtering by source/destination Broadcast storm control Static MAC address forwarding
	Switching	Switching fabric: 144Gbps, non-blocking Max. Frame size: 9 kbytes Forwarding frame: IEEE 802.3, IEEE 802.1q, Ethernet II, PPPoE Prevent the forwarding of corrupted packets
	STP	IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) Multiple Rapid Spanning Tree capability (4 configurable trees) IEEE 802.1s Multiple Spanning Tree Protocol
	QoS	IEEE 802.1p Eight priority queues per port Port-based egress traffic shaping Rule-based traffic mirroring Supports IGMP snooping
	VLAN	Port-based VLAN setting Tag-based (IEEE 802.1Q) VLAN Number of VLAN: 4K, 1024 static maximum Supports GVRP Double tagging for VLAN stacking Protocol Based VLAN Subnet Based VLAN
	Port Aggregation	Supports IEEE 802.3ad; static and dynamic (LACP) port trunking Six groups (up to 8 ports each)
	Port mirroring	All ports support port mirroring Support port mirroring per IP/TCP/UDP
	Bandwidth control	Supports rate limiting at 64K increment
Layer 3 Features	IP Capability	IPV4 support 64 IP routing domains 2K IP address table Wire speed IP forwarding
	Routing protocols	Unicast: RIP-V1/V2, OSPF V2 Multicast: DVMRP, IGMP V1/V2/V3 Static Routing VRRP
	IP services	DHCP relay; VLAN based DHCP server/relay DHCP Snooping
Security		IEEE 802.1x port-based authentication Static MAC address filtering Limiting number of dynamic addresses per port

The following list, which is not exhaustive, illustrates the standards supported in the Switch.

Table 144 Standards Supported

STANDARD	DESCRIPTION
RFC 826	Address Resolution Protocol (ARP)
RFC 867	Daytime Protocol
RFC 868	Time Protocol
RFC 894	Ethernet II Encapsulation
RFC 1058	RIP-1 (Routing Information Protocol)
RFC 1112	IGMP v1
RFC 1155	SMI
RFC 1157	SNMPv1: Simple Network Management Protocol version 1
RFC 1213	SNMP MIB II
RFC 1305	Network Time Protocol (NTP version 3)
RFC 1441	SNMPv2 Simple Network Management Protocol version 2
RFC 1493	Bridge MIBs
RFC 1643	Ethernet MIBs
RFC 1723	RIP-2 (Routing Information Protocol)
RFC 1757	RMON
RFC 1901	SNMPv2c Simple Network Management Protocol version 2c
RFC 2131, RFC 2132	Dynamic Host Configuration Protocol (DHCP)
RFC 2138	RADIUS (Remote Authentication Dial In User Service)
RFC 2139	RADIUS Accounting
RFC 2236	Internet Group Management Protocol, Version 2.
RFC 2338	Virtual Router Redundancy Protocol (VRRP)
RFC 2698	Two Rate Three Color Marker (TRTCM)
RFC 2865	RADIUS - Vendor Specific Attribute
RFC 2674	P-BRIDGE-MIB, Q-BRIDGE-MIB
RFC 3046	DHCP Relay
RFC 3164	Syslog
RFC 3376	Internet Group Management Protocol, Version 3
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMP v3)
RFC 3580	RADIUS - Tunnel Protocol Attribute
IEEE 802.1x	Port Based Network Access Control
IEEE 802.1D	MAC Bridges
IEEE 802.1p	Traffic Types - Packet Priority
IEEE 802.1Q	Tagged VLAN
IEEE 802.1w	Rapid Spanning Tree Protocol (RSTP)
IEEE 802.1s	Multiple Spanning Tree Protocol (MSTP)
IEEE 802.3	Packet Format
IEEE 802.3ad	Link Aggregation

Table 144 Standards Supported (continued)

STANDARD	DESCRIPTION
IEEE 802.3ah	Ethernet OAM (Operations, Administration and Maintenance)
IEEE 802.3x	Flow Control
IEEE 802.3z	1000BASE-X For optical fiber link 1000BASE-SX/LX.

PART VII
Appendices and Index

IP Addresses and Subnetting (345)
Legal Information (353)
Customer Support (357)
Index (363)

A

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

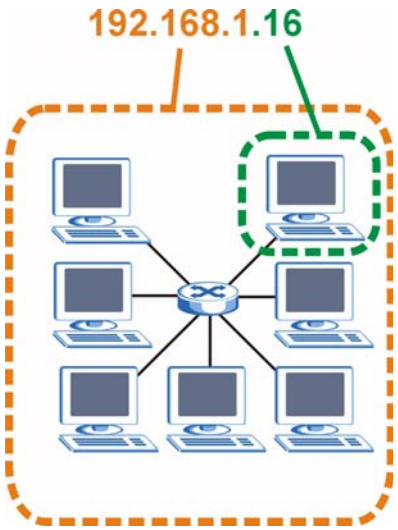
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 210 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term "subnet" is short for "sub-network".

A subnet mask has 32 bits. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 145 IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a "1" value). For example, an "8-bit mask" means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 146 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 147 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} - 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 148 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128

Table 148 Alternative Subnet Mask Notation (continued)

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

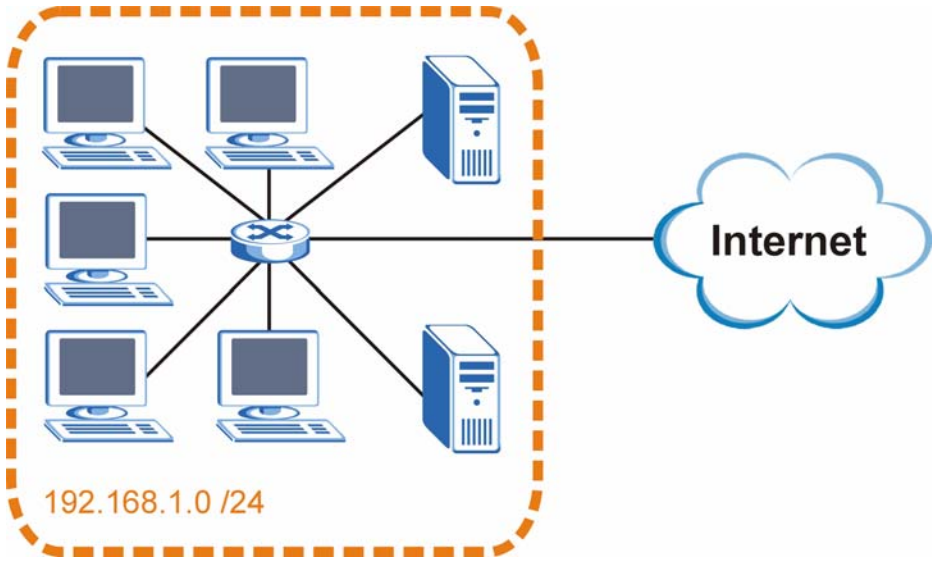
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 211 Subnetting Example: Before Subnetting

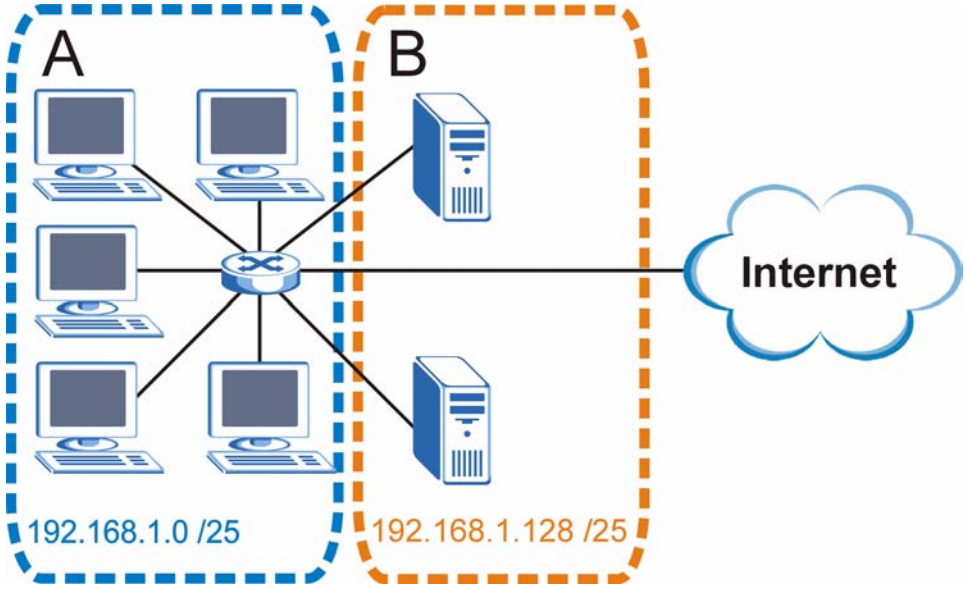


You can "borrow" one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The "borrowed" host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 212 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 149 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 150 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 151 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 152 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 153 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127

Table 153 Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 154 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 155 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6

Table 155 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the Switch.

Once you have decided on the network number, pick an IP address for your Switch that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your Switch will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the Switch unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

B

Legal Information

Copyright

Copyright © 2007 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

FCC Warning

This device has been tested and found to comply with the limits for a Class A digital switch, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this device in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

警告使用者
這是甲類的資訊產品，在居住的環境使用時，
可能造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策.

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CLASS 1 LASER PRODUCT

APPAREIL A LASER DE CLASS 1

PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.

PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating

condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

C

Customer Support

Please have the following information ready when you contact customer support.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

"+" is the (prefix) number you dial to make an international telephone call.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com, www.europe.zyxel.com
- FTP: ftp.zyxel.com, ftp.europe.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: www.zyxel.co.cr
- FTP: ftp.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: www.zyxel.cz

- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

India

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: http://www.zyxel.in
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: http://www.zyxel.com.my
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

North America

- Support E-mail: support@zyxel.com
- Sales E-mail: sales@zyxel.com
- Telephone: +1-800-255-4101, +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.us.zyxel.com
- FTP: ftp.us.zyxel.com

- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

Singapore

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: http://www.zyxel.com.sg
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Thailand

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: http://www.zyxel.co.th
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344-303044, 08707-555779 (UK only)
- Fax: +44-1344-303034
- Web: www.zyxel.co.uk
- FTP: ftp.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)

Index

Numerics

802.1P priority 83

A

access control
  limitations 285
  login account 293
  remote management 300
  service port 299
  SNMP 286
accounting
  setup 192
address learning, MAC 95, 97
Address Resolution Protocol (ARP) 319, 323, 324
administrator password 294
age 122
aggregator ID 135, 136
aging time 78
allowing pop-up windows 328
alternative subnet mask notation 347
applications
  bridging 35
  IEEE 802.1Q VLAN 37
  switched workgroup 36
Area Border Router (ABR) 231
area ID
  and OSPF 237
ARP
  how it works 319
  viewing 319
ARP (Address Resolution Protocol) 319
ARP inspection 201, 203
  and MAC filter 204
  configuring 204
  syslog messages 204
  trusted ports 204
AS Boundary Router 231
authentication 237
  and OSPF 237
  and RADIUS 188
  setup 192
authorization
  privilege levels 194
automatic VLAN registration 88
Autonomous System
  and OSPF 231
Autonomous System (AS) 231, 247

B

back up, configuration file 282
Backbone Router (BR) 231
backbone, routing 231
Backup Designated Router(BDR), and OSPF 232
bandwidth control 339
basic settings 73
BDR (Backup Designated Router) 232
binding 201
binding table 201
  building 201
BPDUs (Bridge Protocol Data Units) 108
Bridge Protocol Data Units (BPDUs) 108
bridging 339
browser configuration 328

C

certifications 353
  notices 354
  viewing 354
CFI (Canonical Format Indicator) 87
changing the password 58
CIST 112
CIST (Common and Internal Spanning Tree) 110
Class of Service (CoS) 251
classifier 151, 153
  and QoS 151
  editing 154
  example 155
  overview 151
  setup 151, 153, 154
  viewing 154
cloning a port See port cloning
cluster management 309
  and switch passwords 314

cluster manager 309, 313
cluster member 309, 314
cluster member firmware upgrade 312
network example 309
setup 312
specification 309
status 310
switch models 309
VID 313
web configurator 311
cluster manager 309
cluster member 309
command interface 38
Common and Internal Spanning Tree (CIST) 110
Common and Internal Spanning Tree, See CIST 112
configuration 228
change running config 281
configuration file 59
backup 282
restore 59, 282
saving 280
configuration, saving 58
console port
settings 47
contact information 357
copying port settings, See port cloning
copyright 353
CPU management port 100
current date 76
current time 76
customer support 357

D

Database Description (DD) 232
daylight saving time 76
default gateway 265
Designated Router(DR), and OSPF 232
DHCP 259
client IP pool 265
configuration options 259
modes 259
relay agent 259
relay example 266
server 259
setup 264
DHCP (Dynamic Host Configuration Protocol) 259
DHCP relay option 82 203
DHCP snooping 201
configuring 203
DHCP relay option 82 203
trusted ports 202
untrusted ports 202
DHCP snooping database 202
diagnostics 303
Ethernet port test 303
ping 303
system log 303
Differentiated Service (DiffServ) 251
DiffServ 251
activate 254
and TRTCM 255
DS field 251
DSCP 251
DSCP-to-IEEE802.1p mapping 256
network example 252
PHB 251
dimensions 335
disclaimer 353
double-tagged frames 167
DR (Designated Router) 232
DS (Differentiated Services) 251
DSCP
DSCP-to-IEEE802.1p mapping 256
service level 251
what it does 251
DSCP (DiffServ Code Point) 251
DVMRP
Autonomous System 247
default timer setting 250
error message 249
graft 248
how it works 247
implementation 247
probe 248
prune 248
report 248
setup 248
terminology 248
threshold 249
DVMRP (Distance Vector Multicast Routing Protocol) 247
dynamic link aggregation 133

E

egress port 102
Ethernet broadcast address 319
Ethernet port test 303
Ethernet ports 43
default settings 44
external authentication server 188

F

fan speed 74
FCC interference statement 353
feature summary 54
file transfer using FTP
  command example 283
filename convention, configuration
  configuration
    file names 283
filtering 105
  rules 105
filtering database, MAC table 315
firmware 74
  upgrade 281, 312
flow control 83
  back pressure 83
  IEEE802.3x 83
forwarding
  delay 122
frames
  tagged 93
  untagged 93
front panel 43
FTP 38, 283
  file transfer procedure 283
  restrictions over WAN 284

G

GARP 88
GARP (Generic Attribute Registration Protocol) 88
GARP terminology 88
GARP timer 78, 88
general features 339
general setup 75
getting help 60
GMT (Greenwich Mean Time) 76
GVRP 88, 93
  and port assignment 93
GVRP (GARP VLAN Registration Protocol) 88

H

hardware installation 39
  mounting 40
hardware monitor 74
hardware overview 43
hello time 122
hops 122
HTTPS 296
  certificates 296
  implementation 296
  public keys, private keys 296
HTTPS example 297
humidity 335

I

IANA 352
IEEE 802.1p, priority 79
IEEE 802.1x
  activate 143, 144, 190, 192
  reauthentication 144
IEEE 802.1x, port authentication 141
IGMP 247
  how it works 244
  overview 243
  port based 245
  setup 245
  version 173
  version 3 245
  versions supported 244
IGMP (Internet Group Management Protocol) 173, 244
IGMP filtering 173
  profile 178
  profiles 175
IGMP snooping 173
  MVR 179
ingress port 102
Installation
  Rack-mounting 40
installation
  freestanding 39
  precautions 40
interface 234
  and OSPF 238
interface, and OSPF 232
Internal Router (IR) 231
Internet
  setting up your browser 330
Internet Assigned Numbers Authority
  See IANA 352
introduction 35
IP
  capability 339
  interface 79, 268
  routing domain 79
  services 339

setup 79
IP multicast example 243
IP source guard 201
ARP inspection 201, 203
DHCP snooping 201
static bindings 201
IP table 317
how it works 317

J

Java permissions 332

L

LACP 133
system priority 137
timeout 138
layer 2 features 339
layer 3 features 339
LEDs 47
limit MAC address learning 148
Link Aggregate Control Protocol (LACP) 133
link aggregation 133
dynamic 133
ID information 134
setup 135, 136
status 134
link state database 232, 234
lockout 58
log 303
login 51
password 58
login account
Administrator 293
non-administrator 294
login accounts 293
configuring via web configurator 293
multiple 293
number of 293
login password 294
loop guard 221
how it works 222
port shut down 223
probe packet 222
loop guard, vs STP 221
LSA (Link State Advertisement) 232

M

MAC (Media Access Control) 74
MAC address 74, 319
maximum number per port 148
MAC address learning 78, 95, 97, 103, 148
specify limit 148
MAC authentication 142
aging time 145
MAC filter
and ARP inspection 204
MAC table 315
how it works 315
viewing 316
maintenance
configuration backup 282
firmware 281
restoring configuration 282
maintenance 279
current configuration 279
main screen 279
Management Information Base (MIB) 286
management port 102
managing the device
good habits 38
using FTP. See FTP.
using SNMP. See SNMP.
using Telnet. See command interface.
using the command interface. See command interface.
using the web configurator. See web configurator.
man-in-the-middle attacks 203
max
age 122
hops 122
metric 236
MIB
and SNMP 286
supported MIBs 287
MIB (Management Information Base) 286
mini GBIC ports 44
connection speed 44
connector type 44
transceiver installation 44
transceiver removal 45
mirroring ports 131
monitor port 131, 132
mounting brackets 40
MSA (MultiSource Agreement) 44
MST Instance, See MSTI 111
MST region 111
MSTI 111
MST ID 111

MSTI (Multiple Spanning Tree Instance) 110
MSTP 107, 109
bridge ID 124, 125
configuration 120
configuration digest 125
forwarding delay 122
Hello Time 124
hello time 122
Max Age 124
max age 122
max hops 122
MST region 111
network example 110
path cost 123
port priority 123
revision level 122
MSTP (Multiple Spanning Tree Protocol) 107
MTU (Multi-Tenant Unit) 77
multicast 173
802.1 priority 175
and IGMP 173
IP addresses 173
overview 173
setup 174, 175
multicast delivery tree 248
multicast group 178
multicast router (‘mrouter’) 248
multicast VLAN 183
Multiple Spanning Tree Instance, See MSTI 110
Multiple Spanning Tree Protocol 109
Multiple Spanning Tree Protocol, See MSTP. 107
Multiple STP 109
Multiple STP, see MSTP 109
MVR 179
configuration 181
group configuration 183
network example 179
MVR (Multicast VLAN Registration) 179

N

NAT 352
network management system (NMS) 286
NTP (RFC-1305) 76

O

OSPF 231
advantages 231
area 231, 237
Area 0 231
area ID 237
authentication 237
autonomous system 231
backbone 231
configuration steps 233
general settings 235
how it works 232
interface 232, 234, 238
link state database 232, 234
network example 232
priority 232
redistribute route 236
route cost 238
router elections 232
router ID 236
router types 231
status 233
stub area 231, 238
virtual link 232
virtual links 240
vs RIP 231
OSPF (Open Shortest Path First) 231

P

password 58
administrator 294
problems 333
PHB (Per-Hop Behavior) 251
ping, test connection 303
policy 159, 160
and classifier 159
and DiffServ 157
configuration 159
example 160
overview 157
rules 157, 158
viewing 160
policy configuration 160
pop-up Windows, allowing 328
port authentication 141
and RADIUS 188
IEEE802.1x 143, 144, 190, 192
MAC authentication 142
port based IGMP 245
port based VLAN type 78
port cloning 323, 324
advanced settings 323, 324
basic settings 323, 324
port details 68
port isolation 93, 102
port mirroring 131, 132, 339

direction 132
egress 132
ingress 132
port redundancy 133
port security 147
address learning 148
limit MAC address learning 148
MAC address learning 147
overview 147
setup 147, 223
port setup 81
port status 67
port VLAN trunking 89
port-based VLAN 99
all connected 102
port isolation 102
settings wizard 102
ports
"standby" 133
diagnostics 303
mirroring 131
speed/duplex 83
power
voltage 75
power specification 335
power status 75
priority level 79
priority, and OSPF 233
priority, queue assignment 79
product registration 355
protocol based VLAN 96
and IEEE 802.1Q tagging 96
example 98
hexadecimal notation for protocols 95, 98
isolate traffic 96
priority 95, 98
PVID 87, 93
PVID (Priority Frame) 87

Q

QoS 339
and classifier 151
queue weight 164
queuing 163
SPQ 164
WFQ 164
WRR 164
queuing method 163, 165

R

RADIUS 188
advantages 188
and authentication 188
Network example 187
server 188
settings 188
setup 188
Rapid Spanning Tree Protocol, See RSTP. 107
reboot
load configuration 281
reboot system 281
redistribute route 236
registration
product 355
related documentation 3
remote management 300
service 301
trusted computers 300
resetting 59, 280
to factory default settings 280
restoring configuration 59, 282
Reverse Path Forwarding (RPF) 248
Reverse Path Multicasting (RPM) 247
RFC 3164 305
RIP
configuration 229
direction 229
overview 229
version 229
vs OSPF 231
RIP (Routing Information Protocol) 229
Round Robin Scheduling 164
router ID 236
routing domain 79, 268
routing protocols 236, 339
routing table 321
RSTP 107
rubber feet 39

S

safety warnings 6
save configuration 58, 280
screen summary 54
Secure Shell See SSH
security 339
service access control 299
service port 300

Simple Network Management Protocol, see SNMP
SNMP 38, 286
agent 286
and MIB 286
authentication 292
communities 291
management model 286
manager 286
MIB 287
network components 286
object variables 286
protocol operations 286
security 292
setup 290
traps 292
version 3 and security 287
versions supported 286
SNMP traps 287
supported 287, 288, 289, 290
Spanning Tree Protocol, See STP. 107
SPQ (Strict Priority Queuing) 164
SSH
encryption methods 296
how it works 295
implementation 296
SSH (Secure Shell) 295
SSL (Secure Socket Layer) 296
standby ports 133
start-up problems 327
static bindings 201
static MAC address 103
static MAC forwarding 95, 97, 103
static routes 227, 228
static trunking example 138
Static VLAN 91
static VLAN
control 92
tagging 92
status 52, 67
LED 47
link aggregation 134
OSPF 233
port 67
port details 68
power 75
STP 116, 119, 123
VLAN 90
VRRP 268
STP 107, 339
bridge ID 116, 119
bridge priority 115, 118
configuration 114, 117, 120
designated bridge 108
forwarding delay 115, 118
Hello BPDU 108
Hello Time 115, 116, 118, 119
how it works 108
Max Age 115, 116, 118, 119
path cost 108, 115, 118
port priority 115, 118
port state 108
root port 108
status 116, 119, 123
terminology 107
vs loop guard 221
stub area 231, 238
stub area, See also OSPF 238
subnet 345
subnet based VLANs 94
and DHCP VLAN 95
and priority 94
configuration 95
subnet mask 346
subnetting 348
switch lockout 58
switch reset 59
switch setup 77
switching 339
syntax conventions 4
syslog 204, 305
protocol 305
server setup 306
settings 305
setup 305
severity levels 305
system information 73
system log 303
system reboot 281

T

TACACS+ 188
setup 190
TACACS+ (Terminal Access Controller Access-Control System Plus) 187
tagged VLAN 87
temperature 335
temperature indicator 74
time
current 76
time zone 76
Time (RFC-868) 76
time server 76
time service protocol 76
format 76
Time To Live (TTL) 249

trademarks 353
transceiver
  installation 44
  removal 45
traps
  destination 291
troubleshooting 327
  accessing the switch 327
  accessing the web configurator 327
  password problems 333
  start-up 327
TRTCM
  and bandwidth control 255
  and DiffServ 255
  color-aware mode 253
  color-blind mode 253
  setup 254
trunk group 133
trunking 133, 339
  example 138
trusted ports
  ARP inspection 204
  DHCP snooping 202
Tunnel Protocol Attribute, and RADIUS 196
Two Rate Three Color Marker (TRTCM) 252
Two Rate Three Color Marker, see TRTCM 252
Type of Service (ToS) 251

U

untrusted ports
  ARP inspection 204
  DHCP snooping 202
user profiles 187

V

Vendor Specific Attribute See VSA
ventilation holes 39
VID 81, 87, 90, 91, 169
  number of possible VIDs 87
  priority frame 87
VID (VLAN Identifier) 87
virtual links 240
virtual links, and OSPF 232
Virtual Router
  status 268
Virtual Router (VR) 267
Virtual Router Redundancy Protocol (VRRP) 267
VLAN 77, 87, 339
  acceptable frame type 93
  automatic registration 88
  ID 87
  ingress filtering 93
  introduction 77
  number of VLANs 90
  port isolation 93
  port number 91
  port settings 92
  port-based VLAN 99
  port-based, all connected 102
  port-based, isolation 102
  port-based, wizard 102
  static VLAN 91
  status 90, 91
  tagged 87
  trunking 89, 94
  type 78, 89
VLAN (Virtual Local Area Network) 77
VLAN number 81
VLAN stacking 167, 169
  configuration 170
  example 167
  frame format 169
  port roles 168, 171
  priority 169
VLAN, protocol based, See protocol based VLAN
VLAN, subnet based, See subnet based VLANs 94
VRID (Virtual Router ID) 268
VRRP 267
  advertisement interval 270
  authentication 269
  backup router 267
  configuration example 272
  Hello message 270
  how it works 267
  interface setup 268
  master router 267
  network example 267, 272
  parameters 270
  preempt mode 270, 271
  priority 270, 271
  status 268
  uplink gateway 271
  uplink status 268
  Virtual Router 267
  Virtual Router ID 271
  VRID 268
VSA 195

W

warranty 354

note 355
web configurator 38, 51
getting help 60
home 52
login 51
logout 60
navigation panel 53
screen summary 54
weight, queuing 164
Weighted Round Robin Scheduling (WRR) 164
WFQ (Weighted Fair Queuing) 164
WRR (Weighted Round Robin Scheduling 164

Z

ZyNOS (ZyXEL Network Operating System) 283